平成 21 年度　経済産業省

地域見守り支援システム実証事業

運用ガイドライン（暫定版）

平成 22 年 3 月

日本システムサイエンス株式会社

まえがき

現在、我が国は、世界で最も速い少子高齢化がすすむ国のひとつであり、医療等を取り巻く環境は、急激に変化している。

現状では、特に地方部での医師不足が加速し、十分な医療サービスの提供が出来ない医療機関の増加や、介護従業者やヘルパーの激減など、医療･介護･福祉体制の地域格差が問題視されている。

他方、都心部でも比較的医療資源はあるものの、核家族化が進み、遠隔地に住む家族との交流や、身近な地域コミュニティの交流の希薄化が相俟って、高齢者等の孤立死の増加など、重要な問題が起きている。

本来、国民は、どこにいても、満足を得られる医療･介護･福祉サービスが提供され、安心して生活を送れるべきであり、現在、このような医療･介護業界の崩壊への早急な対応が求められている。

また、在宅療養者等（高齢者や慢性疾患患者等）が、どのような地域に住んでいても、毎日、安心した生活を送ることができるようになるためには、限られた医療･介護等の資源の中で、効率的で最大限の効果を得るような環境のあり方を考え、「どこにいても、良好かつ多様な医療や介護等のサービスが受けられる環境を整える」ことが必要不可欠といえる。

本事業で追及した地域見守り支援システムの「あるべき姿」が、各特定地域に根付くだけではなく、将来、日本全国、さらには海外へ向けて展開されることを期待する。

目　次

１．はじめに……1

１．１　事業の目的……1
１．２　本運用ガイドライン（暫定版）の目的……1
１．３　運用ガイドライン（暫定版）の作成方針……2
１．４　運用ガイドラインの構成……3

２．適用範囲……4

３．運用の観点から見た地域見守りサービスの特徴……5

４．システム導入に当たっての検討事項……8

４．１　地域見守りサービスの目的、内容……8
４．２　IT 導入の目的……8
４．３　IT 化する情報……9
４．４　利用者の範囲……10
４．５　IT を利用する場所……10
４．６　IT 利用機器……11
４．７　利用者の IT リテラシー……11
４．８　IT 管理者と管理場所……11

５．IT システム運用に当たり考慮すべき事項……13

５．１　契約……13
５．１．１　サービス事業者間の契約……13
５．１．２　サービス事業者と見守り対象者との契約……15
５．２　同意書……17
５．３　見守り支援者の体制……18

６．セキュリティ対策について……19

６．１「地域見守り」特有の留意点……19
６．２　セキュリティ管理における用語および一般的な要件……21
６．３　ネットワーク上のセキュリティの確保……23

７．情報管理……24

７．１　医療に係わる諸記録……24
７．２　情報の発生源別分類……24

７．３　医療情報管理の考え方 24
７．４　アクセス管理 26
７．５　ライフサイクル管理 26
８．システム管理業務 27
８．１　組織・利用者管理 27
８．２　システム維持管理 27
８．３　システム監視業務 28
８．４　バックアップ業務 29
８．４．１　バックアップ方式 29
８．４．２　データ･バックアップ 29
８．４．３　バックアップツールによる管理例 30
８．５　障害時の対応業務 31
８．５．１　障害対策の体制 31
８．５．２　障害防止および発生時の対策 32
８．５．３　障害時の運用 32
８．５．４　障害別対応策 33
９．セキュリティ管理 38
９．１　セキュリティ管理の概要 39
９．２　計画の策定 39
９．２．１　フェーズ１ 40
９．２．２　フェーズ２ 41
９．２．３　フェーズ３ 41
９．３　計画の実施 41
９．４　評価 41
９．５　改善 42
１０．在宅機器の管理 43
１１．運用管理規程について 45
附属書Ａ　セキュリティガイドライン 1
附属書Ｂ　情報資産の明確化 27
附属書Ｃ　リスクアセスメント 31
Ｃ．１ 本附属書の目的 31
Ｃ．２ リスクアセスメントの手法 31
Ｃ．３ 情報セキュリティ基本方針 31

C. ４ リスクアセスメントの実施例 32
附属書 D　運用マニュアル例 45
引用規格･引用文献 46

１．はじめに

１．１　事業の目的

我が国においては、どこにいても、満足を得られる医療･介護･福祉サービスが提供され、安心して生活を送れるような高品質な医療政策が採られてきた。しかし現在、我が国は、世界で最も速い少子高齢化がすすむ国のひとつであり、医療等を取り巻く環境は、急激に変化している。

特に地方部では都市部に増して医師不足が加速し、十分な医療サービスの提供が困難となってきている医療機関が増加していることや、介護従業者やヘルパーの絶対数が不足していることなど、医療･介護･福祉体制の地域格差が問題視されている。

一方、比較的医療資源はあるとされる都心部においても、核家族化が進み、遠隔地に住む家族との交流や、身近な地域コミュニティの交流の希薄化が相俟って、高齢者等の孤立死の増加などの問題が起きている。

高齢者や慢性疾患患者等が、住み慣れた場で安心して療養生活を送れるよう、患者の選択に資するものとして在宅医療が推進されてきたにもかかわらず、このような状況は、とりわけ在宅療養者等にとっては深刻な状況につながりかねない。

在宅療養者等が、どのような地域に住んでいても、毎日、安心した生活を送ることができるようになるためには、「どこにいても、良好かつ多様な医療や介護等のサービスが受けられる環境を整える」ことが必要不可欠といえる。

このような社会の実現に資するものとするために、限られた医療資源･介護等資源を最大限有用に活用し、在宅療養者等が真に必要とするサービスを、効果的かつ永続的に提供でき得るサービス基盤の確立に向けた事業を「地域見守り支援システム実証事業」として開始したところである。

１．２　本運用ガイドライン（暫定版）の目的

システム、という語から直ちに想起されるのは「情報システム」のことであるかもしれない。確かに、医療･介護、健康関連サービス事業者、行政等の関係者による有機的な多職種連携を形成し、これを通じて地域見守りサービスの効果を最大限に発揮するために、IT の活用は、最も有効な手法の一つであり、このメリットを極大化するため「地域見守り支援システム実証事業」においては、より効果的な IT の活用方策について検証することを事業目的の一つとしている。しかし本事業に言うシステムには、そのような情報システムを効果的に用いて、持続可能かつ良質な地域見守りサービスを提供し得る「社会システム」という意味合いもある。

そのような観点も考慮して、本ガイドラインは、地域見守りサービス事業者が、地域見守りという社会基盤において実際に情報システムを利用してサービスを提供しようとするとき、遵守すべき事項及びその考え方を示そうとするものである。

１．３　運用ガイドライン（暫定版）の作成方針

「地域見守り支援システム」の基盤構築には、サービスを受ける対象者を取り巻く、医療・健康・介護等にまつわる事業者が連携・協働して当たることが必須となり、ITを活用して、その連携・協働をより効果的・効率的にしようとするものである。

そうすると、それら関係者間で共有・交換される情報にあっては、いわゆる医療情報・健康情報・介護情報が明確な区別なく取り扱われる可能性がある。

これらは個人情報のうちでも、もっともセンシティヴ性が高いとされる情報であり、その取り扱いには特有の難しさを伴う。個人情報保護法の制定時にも医療分野の個別法にかかる検討をせよとの付帯決議がなされたことからもそれは明らかである。

これに対しては同法の執行指針として「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」が公表されており、この中で情報システムを用いる場合には「医療情報システムの安全管理に関するガイドライン」を参照すべきと示されている。

このようなことを背景に、本ガイドラインを纏めるにあたっては、いくつかの論点を整理しておかねばならなかった。

第 1 に、医療情報には先述のような厳しい要件を課したガイドラインがあるが、健康情報、介護情報にはそのようなものがないと考えられがちな点である。

我が国の法令やその指針においては、情報取扱者の有する資格や職責、機関の設置の根拠となった法規等により、その適用の可否が区分されているものが多くみられる。

第 2 に、多数の関係者の連携・協働においては、共通理解を形成する上で、標準規格を示し、これを遵守することが、情報安全（ひいては患者安全につながることも多い）のための方策についての説明責任を果たすことを容易にするため、本ガイドラインにおいても ISO(International Organization for Standardization ; 国際標準化機構) TC(Technical committees) 215（「Health informatics」）による国際標準等を多数参照することとなる。

英文で書かれたこれらの規格においては、医療情報・健康情報・介護情報等の区別が無く、統合的に"Health information"や“Healthcare Information”という言葉がよく用いられる。これを単に「健康情報」と翻訳してしまうと、先の論点とは逆に、医療情報とは様々な点において質が異なるのではないかという議論が起きそうである。

しかしサービス利用者からしてみれば、医療情報と呼ばれようが健康情報と呼ばれようが、また介護情報と呼ばれようが、取り扱われる情報が本人にとっては一連の、不可分のものであり、それが身体状況にまつわる情報である限りは同程度に機微である可能性もある。そのような立法上の理由や行政における区別等によって、情報の取り扱いに厳格さが要求される関係者と、そうでない関係者がいるということは理解し

にくい。本事業のような、さまざまな職種の連携により進められる事業においては、利用者の情報保護や適切な書類の電子化のための法令・指針等を関係者の共通理解として、遵守することが期待されている。

個人が安心して療養生活を送れるようにとの観点から、本人の生活状況も踏まえた情報の収集、蓄積、伝達、活用を事業として実証するにおいては、それらは整理、分類、統合を繰り返しつつ、本人に最適なサービスがなされるよう活用される。

そうすると、先述するような狭義に捉えることが必ずしも妥当しない場面が生じるため、本ガイドラインを纏めるにあたっては、利用者の医療情報・健康情報・介護情報等と区別するのではなく、統合的にヘルスケア全般に関わる情報とでも広義に捉えておかないと、種々の不都合を生じるおそれがある。

したがって、情報システムにかかる要件定義書とも位置付けられる本ガイドラインは「医療情報システムの安全管理に関するガイドライン」を参照することを一応の基本とし、地域見守りサービスの提供の実態を把握して課題を検討しつつ具体的には次の手順に従った。

① モデルシナリオの作成
② 業務フローの分析
③ IT システムへの展開（機能要件の具体化）
④ 要求仕様書（暫定版）、運用ガイドライン（暫定版）を作成

それにより、地域見守り支援システムにかかる以下の項目の整理、検討を行った。

・情報共有の仕組み、データセット等の整理･検討
・セキュリティ機能の整理･検討
・運用ルールの整理･検討

これらは、これから地域見守り支援システムを利用して地域見守りサービスを提供しようとする事業者が、そのシステムの運用にあたり参照されるべき標準的な運用ルールとなることを目指すものである。

１．４　運用ガイドラインの構成

本運用ガイドラインは以下のように構成されている。

① 運用の観点から見た地域見守りサービスの特徴
運用ガイドラインに記す各種運用業務の前提として認識しておくべき地域見守りサービスの特徴について記している。

② システム導入に当たっての検討事項
地域見守り支援システムの導入（システム構築及び運用）に当たって、事前に検

討しておくべき項目について述べている。

③ IT システム運用に当たり考慮すべき事項
運用ガイドラインでは主に IT システムの運用に関する事項について述べているが､それに関連して IT に直接関係はないが考慮すべき事項について述べている。具体的には、契約のこと、同意書、及び見守り支援者に体制などである。

④ セキュリティ対策について
地域見守り支援システムの運用に当たり必要なセキュリティ対策について､「地域見守り」特有の留意事項、セキュリティ対策実施に当たり必要な概念・用語、セキュリティ・リスク及びそれに対するセキュリティの確保、などについて説明している。

⑤ 情報管理
地域見守り支援システムで取り扱う情報の種別と取扱い方法､情報管理の考え方、さらに情報のアクセス管理、ライフサイクル管理について記している。

⑥ システム管理業務
地域見守り支援システムの維持管理に必要な業務について記している。

⑦ セキュリティ管理
PDCA サイクルに基づくセキュリティ管理の基本的手法について述べている。具体的な知識等は附属書に示した。「附属書 A セキュリティガイドライン」で ISMS（情報セキュリティ管理システム）の考え方と方法を提示、具体的なセキュリティ評価の検討例として「附属書 B 情報資産の明確化」､「附属書 C リスクアセスメント」を記載した。

⑧ 在宅機器の管理
地域見守りにおいて使用される在宅機器の管理について述べている。安否確認、バイタルセンサやそのデータの収集・送出機器などである。
今年度は一応内容を記述しているが、暫定記述である。正式には来年度充実させる予定である。

⑨ 運用管理規程について
ここも暫定記述｡来年度､地域実証事業での知見も入れて充実させる予定である。

２．適用範囲

本書は、医療･介護･福祉のサポートを必要とする見守り対象者に対する地域見守り支援システムの要素機能として考慮すべき要求事項について規定する。在宅医療･介護･福祉サービスの連携を支援する情報共有システム･IT ツールに適用される。

３．運用の観点から見た地域見守りサービスの特徴

運用の観点から見た地域見守りサービス及び地域見守り支援システムには以下の特徴がある。

（１）多様なサービス

- 要求定義書に示したように、見守り対象者（在宅療養者等）の状態によって提供するサービスも様々である。単に「声かけ」や「安否確認」のみのサービスでよい場合もあれば、医療を伴う場合、介護を伴う場合、あるいは両方のサービスを提供する場合もある。また、見守り対象者宅のバイタルデータ収集サービスがあるなど、様々である。

（２）多様な利用者

- 多様なサービスに関連して、地域見守り支援システムの利用者も多様である。
- 利用者には、見守り対象者本人や家族も含まれる。

（３）多職種連携

- それらの人たちが単独でシステムを利用することは少なく、一般にそれぞれの人たちが連携してサービスを提供する。すなわち、医療、介護分野の多様な職種の人たちが協力して見守りのサービスを行う。
- さらに、時間の経過に伴って見守り対象者の状態が変わることにより提供するサービスも変わっていくが、それに伴い関わる職種も変化していく。

（４）職種ごとの規制

- 各職種に適用される法律すなわち規制は多様である。
- 医師には医師法、歯科医師には歯科医師法、看護師には保健師助産師看護師法、介護士には社会福祉士及び介護福祉士法、ケアマネジャー（介護支援専門員）は介護保険法、ホームヘルパーも介護保険法、薬剤師は薬剤師法、理学療法士、作業療法士は理学療法士及び作業療法士法、栄養士は栄養士法、民生委員は民生委員法、自治体職員には地方公務員法など、多様である。
- 一般に、法律に定められた国家資格、公的資格には、それぞれ秘密保持義務が課せられているが、その程度、罰則の有無等は多様である。
- また、地域見守り支援システムの利用者になる可能性のある家族、見守り対象者本人には、上記のような規制はない。
- 将来的に、見守りシステムを利用する可能性のある隣人、友人あるいはボランティアの人々についても、特段の規制はない。

（5）情報を利用する場所

- 地域見守りサービスは、特定の施設におけるサービスに限定されないので、情報を利用する場所も多様である。
- まず、病院・診療所あるいは介護施設は当然として、見守り対象者の居宅もあるし、地域見守りセンターのような施設があれば、そこも利用場所である。
- また、各種施設から見守り対象者宅への移動中における利用も考慮する必要がある。
- 情報の利用には、情報の入力及び参照があり、それぞれの作業を行う場所が異なることもある。
- それぞれの利用場所に応じて、ネットワーク環境は様々であるし（ネットワーク環境が得られないところではオフラインで作業することもあり得る）、オープンな場所で作業する場合には第三者に見られるという可能性についても考慮しなくてはならない。

（6）情報を保存する場所

- 利用する場所とともに、情報を保存する場所も地域見守りの場合は一般に多様である。情報の保存をセンターで集中して行う場合は比較的簡単であるが、分散しておく場合は、それぞれの置き場所での責任ということを考慮しなければならない。
- また、センターで集中して管理する場合でも、各種の情報をまとめて管理する場合、その情報の管理に誰がいったい責任を持つかということを明確化しておく必要がある。まとめた全体は誰、そのうちのこの部分は誰、外の部分は誰、というように責任を明確化する。特に責任分界点の観点から、責任のすき間がない様にしなくてはならない。

（7）情報を利用する機器

- 病院・診療所あるいは介護施設などの閉じた施設内ではパソコン等を使用するのが一般的であろう。ただし、担当者間での直接的な連絡には電話を使うこともある。
- 見守り対象者宅やその道中で見守りサービス提供者が使用する機器は、パソコンの可能性もあるが、携帯電話や PDA などのモバイル機器を使う可能性も大である。
- 見守り対象者が自宅で使う機器としては、パソコンもあるが、テレビを端末として使う場合もある（特にケーブルテレビを利用した見守りサービスの場合）。

・ バイタルデータ収集はそれぞれ専用の機器を使う。ただし収集したデータをセンターに送るときは、直接ネットワークを経由して送る形もあるが、パソコン等を利用して、途中人手を介して送る場合もありうる。

（8）利用者の IT リテラシー

・ 利用者として様々な職種が関わるが、それら職種間、あるいは職種内でも IT を利用する能力のバラつきは様々である。システムはそれらの状況を考慮して構築する必要がある。また、教育を行ってリテラシーの底上げを行うことも重要である。

４．システム導入に当たっての検討事項

前章のサービス及びシステムの特徴を前提に地域見守り支援システムを構成していくことになるが、IT システム導入に当たっては、システム導入の前に事前に検討すべき項目がいくつかある。

検討を要する項目は以下のようなものである。

（１） 地域見守りサービスの目的、内容
（２） IT 導入の目的
（３） IT 化する情報
（４） IT を利用する場所
（５） IT 利用機器
（６） 利用者の範囲
（７） 利用者の IT リテラシー
（８） IT 管理者と管理場所

以下それぞれの項目について、具体的な内容、検討の進め方について述べる。

４．１　地域見守りサービスの目的、内容

あらためて言うまでもないが、IT 導入を検討する以前に、提供しているあるいは提供しようとしている見守りサービスの目的、内容について明確化しておく必要がある。また、どのような人を見守り対象者としているかも重要である。

これがはっきりしていないと、IT の導入を進めるにしても、IT でやるべき内容を明確化することができない。またこれを中途半端なままに IT システムを構築してしまうと、使いにくいシステム、あるいは役に立たないシステムが出来てしまう可能性が大きい。

地域見守りサービスの目的、内容の明確化を指南することは、本地域見守り支援システム運用ガイドラインの範囲を越えることであるが、別冊の地域見守り支援システム要求定義書に一部関連情報を記してあるので、必要ならば参考にしていただきたい。また、在宅医療、介護関連の書物、インターネットの情報なども参考になろう。

以上を受けて、以下の項目の検討に進んでいただきたい。

４．２　IT 導入の目的

地域見守りの目的、内容が明確になっている前提で、次に IT 導入の目的について検討する必要がある。

IT 導入の目的は、二段階で考える。

まず、IT 導入の背景となる課題は何かを明らかにする。つまり、情報の収集、共有、

連絡など、情報の取扱いになどを明らかにすることである。課題によっては表面上情報の取扱いに関係ないように見えても、情報の取扱い方法を改善することにより課題を解消ないし緩和することが出来るので、それらについて検討の対象とする必要がある。

次に、IT 導入によってそれらの課題をどのようにして改善しようとしているのかを明確化する。つまり、課題に対する解決手段・方法である。また、IT を導入するとしても解は一つではなく、外部仕様によりさまざまな方式があり得ることから、必要に応じて目的の中に入れて考える必要がある。

典型的なものとして、例えば見守り対象者を取り巻く複数のサービス提供者間の連絡ないし情報共有の問題がある。見守り対象者の情報を IT システムに記録し、サービス提供者間の情報共有を行うことは地域見守り支援システムの重要な目的の一つである。

その他、見守り対象者や家族への情報提供、見守り対象者の身体情報のモニタリング等も、重要な目的になる。

なお、IT 導入によって地域見守りサービスの内容が変わり、その結果最初の「地域見守りサービスの目的、内容」も変化することがあり得る。したがって、本章で述べていることはワンパスで終了する話ではなく、何度かループして検討を行い、全体として最適な計画を作るべきである。

さらに、計画を作ったらそれで終わりというわけではなく、システム開発の過程やシステム開発後の運用の過程で繰り返し評価を行い、得られた知見をフィードバックして「地域見守りサービスの目的」や「IT 導入の目的」、その他の事項のブラッシュアップをはかり、より適切なシステムにしていく努力も必要である。

４．３　IT 化する情報

次に IT システムで何を情報として取り扱うかを明確にする。

上記の IT 導入の目的に関わることであるが、その目的に沿って IT システムで取り扱う情報を明確化する。

とは言え、すべての情報を IT システムで取り扱わなければならない、というわけではない。それまで紙で扱っていた情報を IT 化しようというとき、すべてを IT 化することが良いかどうか、慎重に考える必要がある。場合によっては、また IT システムの導入にあたっては、紙のまま残したほうが良い情報もあるかもしれない。また、それまで全体的には一つの情報として扱っていたものを、ある範囲は IT 化し、残りは紙のまま残す、という判断もありえる。

それまで口頭で交換していた情報がある。対面で交わす情報交換、電話による情報交換などである。口頭による情報交換の特性は、即時性（リアルタイム性)、直接性である。状況によるが、口頭による情報交換では、一般的にその場で回答が得られる利

点がある。

一方、IT システムを利用する場合、電子メールや共有メモリ、共有データベースの利用などでは、即時性、直接性はないが、逆にそのような特性を利用する必要がないときは有効である。この場合は、情報交換の記録が残るという利点がある。

IT システムとの連続性を保つため、対面ないし電話による情報交換においても、交換した情報、もしくは交換したという事実をシステムに記録しておくことがのぞましい。

以上、どのような情報を IT 化すべきかという観点で述べたが、さらに扱う情報の中身の検討も必要である。氏名、住所、年齢などの個人の基本情報、医療情報、介護情報などがあるが、さらにその中身についても IT 化の範囲を検討する必要がある。

その他、バイタル測定機器などで発生するデータなどもある。

４．４　利用者の範囲

IT システムを構築したとして、その利用者は誰か。

見守り対象者の周囲で見守り対象者の支援を行う人々が利用者の候補となるが、どこまでの範囲の人々を利用者とするか。IT システムの目的、具備機能により決定する。

具体的には、見守り対象者本人、家族、医師、看護師、ケアマネージャ、介護士、ヘルパー、民生委員、隣人、ボランティア、あるいは行政機関の関係者などがある。目的、提供機能によって範囲を決定するが、もう一つ、本ガイドラインでも詳述しているが、個人情報保護の問題についても考慮しなくてはならない。

見守り対象者に関する情報は、医療情報を筆頭として対象者にとって最高機密の情報であることが多い。したがって、むやみに利用者の範囲を広げると、情報漏洩の問題が発生する。

情報漏洩の問題としては、最近世情を騒がしているネットワーク経由で情報を漏洩したとか、パソコンを紛失したため情報漏洩が発生したなどの問題もある。しかし単に本来見る理由がない、あるいは権限がない人が情報に接触することによって、予期せぬトラブルが発生することもある。

したがって、IT システムの利用者の範囲は慎重に決める必要があるし、さらに利用者の範囲に入っている人でも、すべての情報に自由にアクセスできるわけではなく、種々の条件に基づき、利用者のアクセス権限を決めてシステムを運用しなくてはならない。

４．５　IT を利用する場所

主にセキュリティに関係することであるが、IT システムをどこで利用するか、あらかじめ明確化しておく必要がある。

具体的には、医療機関、訪問看護ステーション、在宅介護支援センターなどの拠点、

見守り対象者の居宅、あるいは拠点から対象者居宅への道中の車内、などが考えられる。それぞれによって考慮すべきセキュリティ要件も異なってくる。

４．６　IT 利用機器

情報共有・交換を支援する機器としては、パソコン、携帯電話などがある。また、見守り対象者宅、及び対象者宅への道中で、オフラインで PDA（携帯情報端末）などを使用することもあり得る。

これもやはりセキュリティに関連した検討事項である。簡単に他人に使用できないようにすること、紛失した場合の対応方法などを検討しておく必要がある。

４．７　利用者の IT リテラシー

今日でも、誰もが IT 機器を自由に使えるわけではない。

医療分野では、レセコン、オーダリングシステム、電子カルテシステムが次第に普及しつつあるが、すべての関係者が IT 機器を使えるというわけではない。

介護分野では、介護保険請求が IT 化されているので、その範囲では IT 利用は必須であるが、見守り対象者を直接支援する立場のヘルパーの方々などは、その枠外である。

また、近年の携帯電話の爆発的普及により、若い人々は IT 機器に対するアレルギーはなくなっているが、誰でもどんな IT 機器でも使えるというわけではない。

そのような背景を前提に、まず利用者の IT リテラシー、すなわち IT 利用能力を明らかにし、IT システムの開発に当たっては、こうした状況を前提に、使いやすいシステムの機能を実現していく必要がある。

また、利用者に対する教育も重要である。

このシステムは何のためにあるか。どのようにして使用し、何が出来るようになるかを、しっかり利用者に伝える必要がある。

４．８　IT 管理者と管理場所

一般に地域見守り支援 IT システムは、24 時間、365 日休みなく動かす必要がある。その運用管理の任に当たる IT 管理者を決めておかなくてはならない。さらに、大きなシステムの場合は、その下で実際の作業を行う体制もしっかり組織しておく必要がある。IT 管理者はまた、システムのセキュリティについても十分配慮すべきである。

支援システムの形態としては、地域の中心にセンターを置いて、そこにサーバなどセンター機器を集中しておくやり方がある。一方、関連サーバを、医療機関、訪問看護ステーション、在宅介護支援センターなどそれぞれの拠点に分散しておく形態もある。この場合はそれぞれの拠点ごとに IT 管理者を定めるだけでなく、拠点ごとの IT 管理者間の連絡網を形成し、何か事故が起きたときに即時に対応できる体制を作って

おく必要がある。

サーバなどの IT 機器を置く物理的場所も重要である。出来ればみだりに関係のない人間が近づけるような場所におくべきではなく、止むを得ずオープンな場所に置くときでも、関係のない人間が簡単に触れないようにしておくべきである。

端末機器については、管理場所の限定は簡単ではないが、その場合でもセキュリティレベルが保たれている場所で使用する際の機能、またそうではない場所で使用する際の機能を分けるなど、セキュリティに関して配慮すべきである。

５．IT システム運用に当たり考慮すべき事項

本運用ガイドラインは、地域見守り支援システムすなわち IT システムの運用に関する事項を記載することが目的であるが、その前提として、IT システムの操作には直接関わらないが考慮すべき事項がいくつかある。

５．１　契約

地域見守りサービスは一般に、地域の見守り対象者を複数の支援者で見守るサービスである。したがってそこには、サービスの中核となるサービス事業者と、その周りで共同してサービスを提供する組織、支援者がいる。医療機関（病院、診療所、訪問看護センター、薬局等)、介護事業者、行政機関、民間事業者などである。

共同して事業を行うからには、一般的には中心となるサービス事業者と、共同してサービスを提供する組織の間に何らかの契約が存在するのが通常である。IT システムを使う以上当然ながら、その契約中には IT に関する事項も含む。

一方、サービスを受ける見守り対象者もサービス事業者との契約に基づいてサービスを受けることになるが、IT を前提とするサービスを受ける以上、その契約書には IT に関する事項もある。

以上二形態の契約書に関して、IT について考慮・記載すべき事項について、以下に記す。

５．１．１　サービス事業者間の契約

まず、IT システム以前に、相互に協力して提供するサービスの内容とその分担、責任範囲を明らかにする必要がある。

その上で IT システムに関して規定すべき項目としては、以下のようなものがある。

（1）IT システムの利用目的

協力して提供する地域見守りサービスにおいて、IT システムの利用目的を明示する。具体的には、例えば多職種連携のための情報共有、安否確認機能、バイタルデータ収集機能、ないしは一般的な情報提供機能などとなろう。

（2）共有する情報

地域見守り支援システムで関連職種で情報共有を行う場合、どんな情報を共有するかを明らかにする。

共有しない情報は契約書に明示する必要はないが、見守りサービスを地域で円滑に実施するために、それぞれどんな情報を保有しているかを必要な範囲で相互に明らかにしておくと良い。

（3）アクセス制御

共有情報のアクセス制御に関する条項。

個別の見守り対象者に対する各支援者のアクセス権は次の見守り対象者との契約（もしくはその附属書）に記すが、そのもととなる考え方などを記す。通常この考え方はアクセスポリシー、もう少し広くはセキュリティポリシーに記すので、それを参照・添付するか、関連記述を転記することになる。

（4）IT システムに関する管理者とその役割

それぞれの IT システムの管理者ないしは責任者を明らかにすることを条項に入れる。またその役割についても記す。

なお、通常具体的な管理者の指定については契約書とは別に行う（さもないと管理者が代わる度に契約書を改定しなくてはならない)。

（5）管理者の責務

それぞれの IT システムが支障なく運用される環境を整備すること、コンピュータウイルス等によるセキュリティ脅威に対して安全を確保すること、機器やソフトウェアに変更があった場合でも情報が継続的に使用できるように維持すること、アクセス権限の設定と利用者管理、操作手順書の整備と利用者教育、苦情受付窓口の設置と維持管理、などについて規定する。

（6）IT システムの利用者

共同で使用する IT システムの利用者を明示することを規定する。
利用者は変動する可能性があるので、管理者の場合と同様、具体的な利用者名は契約書とは別に指定する。

（7）利用者の責務

利用者アカウント情報等の管理について規定する（他者に使用させない、他社と共有しない、等)。また、入力情報に関して責任を有すること、アクセス権限外の操作や参照した情報の目的外への利用の禁止、見守り対象者の個人情報保護の観点からプライバシーの侵害の禁止、などについて記す。

（8）ネットワーク接続、利用機器

相互の IT システムのネットワークによる接続方法、また使用する IT システムで利用する機器、ソフトウェアなどを、必要な範囲で規定する。

（9）機密保持、セキュリティ

一般に地域見守りサービスにおける見守り対象者の個人情報は、機密扱いとして保護すべき情報である。また、共同サービス事業やそれぞれの組織、IT システムの運用体制、運用方法なども、みだりに外部に漏洩すべきことではない。場合によって、それらの情報が漏洩することによって、事業や IT システムに脅威が及ぶこともある。さらに、当然のことながら、IT システムのセキュリティにも配慮が必要である。

以上のような項目について規定する。

（１０）異常時の対応

IT システムに異常が生じたときの対応、その後の連絡方法、責任分担等を記す。

以上は例示であり、このほかにも IT について契約書中に盛り込むべき項目があり得る。具体的なサービス、システム及びその運用の内容に応じて項目設定していただきたい。

なお、上記のうち、（3）、（9）、（１０）はセキュリティ関連の項目である。セキュリティ関連については、これ以外も含めて網羅的に規定されている。詳細については９章及び付属書 A～C を参考にしていただきたい。

以上の事項に関し、個々の契約書中に記すのも一法だが、一般に IT システムについてその管理に関して運用管理規程（１１章参照）を規定するのが通常であるので、その規程中に関連項目をまとめて規定し、契約書中からその運用管理規程を参照する形にする方法もある。

５．１．２　サービス事業者と見守り対象者との契約

医療では一般に見守り対象者すなわち患者と医師との間で契約書を取り交わすことはない。通常は口頭で契約が成立したとみなされる。ごく特別な治療を施す場合に同意書をとるということがあり、それは契約書の一種とは言えるが、一般的には契約書はない。

介護の場合は、介護サービスの申請をして、認定を受け、など、必要な手続き後、最終的には介護サービス提供者とサービス受益者間で契約書を取り交わす。福祉サービス、健康サービスもこれに準じ、契約書を取り交わしたあとサービスを開始する。地域見守りサービスも、この介護サービスの提供形態に準ずると思われ、契約書を取

り交わしたあと、サービス・インする。
したがって、IT を利用するサービスを提供する場合には、一般に IT に関する条項を契約書に追加する必要がある。もちろん、契約書に追加するだけでなく、きちっと対面でその内容について説明する必要があることは言うまでもない。

要求定義書に記したシステム機能を併用して見守りサービスが提供されることになるが、その要求定義書で定義しているシステム機能のうち、平常の見守りサービスで使用されるシステム機能は、サービス提供支援機能とセンシング支援機能である。ニーズキャッチ機能、サービス提供支援機能は、見守りサービスを提供するに当たり、そのサービス内容などを決めるために用いられる。サービス契約はその後締結される。したがって、契約書に盛り込まれる IT 関連条項は前記のサービス提供支援機能とセンシング支援機能に関するものとなる。
以下、それぞれの機能に関連して契約書の IT 関連条項に盛り込むべき事項について述べる。

（1）サービス提供支援機能関連
本機能は具体的に、サービス提供記録管理機能、チームケア支援機能、遠隔サービス提供機能からなる。その中核は、関連職種による情報共有である。
そこで見守り対象者との契約において必要となる事項は、まず、見守りサービスに伴う関連職種による情報共有に対する同意、ついで必要ならば情報共有に関わる職種ないし具体的な人の指定（ただし具体的な人の指定は契約書とは別の様式で取り交わしたほうが良い。サービスの途中で変わる可能性もあるので。）、及び情報共有に関わる職種ないし具体的な人のアクセス権の指定（同様に具体的な人に関しては別様式で指定する）、などである。

（2）センシング支援機能関連
本機能には、IT 機器などを使用した安否確認機能、声かけ機能、服薬や通院のリマインド機能、バイタルセンサなどによるバイタルデータ等管理機能、及び緊急通報機能がある。いすれも見守り対象者の個人情報を IT システムに格納するとともに、その経時的な状態情報を逐次記録し、担当者ないしアクセス許可された人が適宜参照して状況を確認する。
したがって、情報の記録と参照に関する同意を契約書に記入する必要がある。
また、安否確認機能等においては、見守り対象者のプライバシーを一部侵害する可能性があるので、その点に関する同意も必要である。

以上は、見守りサービスに伴うシステム機能に直接関連する事項であるが、その外

にも以下の点について記載する必要がある。

（3）見守り対象者または同家族によるシステムの利用

見守り対象者または同家族が、サービスを実施する支援者と同等の立場でもしくはそれに準ずる立場でシステム機能を利用することがある。

この場合は、対象者または家族によるシステムの利用を許諾する旨を示す条項と、利用時に遵守すべき事項を記載する。後者に関しては、前記のサービス事業者間の契約に記載している利用者が遵守すべき条項を準用する。

（4）サービス事業者の責務

サービスを提供する立場から、その責務について記載する。

IT システムに関しては、個人情報の保護、情報の保全、サービスの継続、異常時対応などについて記載する必要がある。また何らかの事由により IT システムに関して損害が発生したときその賠償、逆に損害が発生したときの免責事項なども記載する。

また逆に、地域見守り対象者側によるシステムの利用において、地域見守り対象者側の不手際により IT システムに損害が発生した場合の賠償に関しても、記載する必要がある可能性がある。

なお、この契約では、見守り対象者側の契約者はまずは見守り対象者自身であるが、見守り対象者の高齢ないしはその他の要因（認知症等）により、見守り対象者の周辺にいるキーパーソン（一般に家族）が契約者になることもある。ただし、見守り対象者と家族等とは利害が一致していないことがあるので、注意が肝要である。

５．２　同意書

通常、見守り対象者に対するサービスの大枠は契約書に記載されるが、サービスの途中でサービス形態が変更されることがあり、その場合には見守り対象者から同意書を取ることによりその変更内容を確認することもある。

IT システムに関して同意書を取って運用する事項には以下のようなものがある。

（1）見守りサービスの変更

見守りサービスの変更は再契約が望ましいが、マイナーな変更の場合は同意書で行うこともあり得る。

（2）IT システムに関係するものとしては、センシング支援機能の開始または終了など。地域見守りサービス提供者（支援者）すなわち IT システムの利用者の設定及び変更。

（3）IT システムの共有情報のアクセス権の設定及び変更

アクセス権の設定ないし変更は（2）と同時に行われることもあるが、利用者は変更せずにアクセス権のみ変更することもあり得る。

なお、緊急時においてはこの限りではない（6．1節（6）参照)。

5．3　見守り支援者の体制

個々の見守り対象者へのサービスに当たり、支援者側は一般にチーム体制を組んでサービスを行う。チーム体制の編成は暗黙的になされることもあるが、一般的には明示的にチーム編成を行うことが望ましい。チーム構成員は誰で、リーダは誰である、というようなことである。また、チーム構成員の誰かが病気その他の要因で欠けたときの代行者を決めておく必要もあるし、チーム員それぞれの間の連絡手段も明らかにしておく必要がある。

IT システムを使用する場合は、情報共有の関係上、見守り対象者側の指示に基づき（積極的な指示はない場合もあるが、その場合でも事前の説明により意思決定していただく)、該当の見守り対象者の情報に対して誰がどの情報にアクセスできるようにするか、情報の利用者とアクセス権を決定しておく必要がある。

この、利用者とアクセス権の決定に関して、おのおのの見守り対象者ごとに誰か統括管理者を1名決めておくことが望ましい。また、この統括管理者は、地域見守りサービス自体の該当見守り対象者に対するサービスの統括責任者があらかじめ決められている場合は、それと同一であることが望ましい。

支援者すなわち IT システムの利用者の変更ないしアクセス権変更の必要が生じたときは、通常はこの統括管理者が判断して処置を行う。

なお、緊急時はこの限りではない（6．1節（6）参照)。

６．セキュリティ対策について

地域見守り支援システムは情報処理システムの一種であるので、セキュリティ対策に万全を期さなくてはならないのは言うまでもない。

一般的にセキュリティ対策とは、情報、ハードウェア、ソフトウェアなどの資産を安全に保つための個々の対策のことである。例えば、情報漏洩を防ぐための利用者認証、コンピュータウイルス対策、データのバックアップなどのことである。

地域見守りサービス及び地域見守り支援システムでは、見守り対象者への適切なサービスを行うため、医療情報を含む見守り対象者の個人情報を取り扱うことが想定される。見守りの情報は個人にとって機微な情報であり、それを取り扱う事業者に対しては、取り扱いに特段の注意を払うことが法律上求められている。そのために適切なセキュリティ対策を実施することは必要不可欠の要件である。

さらに、誤りのないサービスを提供するための情報の完全性の維持や、有効なサービス提供のための可用性の維持、例えばシステムやネットワークの安定稼働・性能維持、トラブル発生時の迅速な復旧対応なども求められる。これらもセキュリティ対策に含まれる。

以上に関する具体的なセキュリティ対策手法については９章及び附属書A、B、Cに記すが、ここでまずその前提として「地域見守り」特有の留意点について記す。

６．１「地域見守り」特有の留意点

（１）医療情報と同様の配慮が求められる点

- 厚生労働省から公開されている「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」では介護分野も医療分野と同様に個人情報の取り扱いが求められる分野とされている
- その中では、「個人情報取扱事業者としての法令上の義務等を負わない医療・介護関係事業者にも本ガイドラインを遵守する努力を求めるもの」としており、小規模事業者もガイドライン遵守が求められている
- さらに、「当該患者・利用者が死亡した後においても、医療・介護関係事業者が当該患者・利用者の情報を保存している場合には、漏えい、滅失又はき損等の防止のため、個人情報と同等の安全管理措置を講ずるもの」としており、利用者の死亡後もその情報管理に同等の対応を求めている

（２）関係者が複数、規模・職種が多様な点

- 対象者が入院あるいは通院している医療機関、対象者が介護を受けている介護

事業者、情報を保存しているデータセンタやネットワーク事業者、公的機関、地域住民、対象者の家族などが関係者となる
- それぞれの職種ごとに適用される法律や規制が異なる。
- つまり同じ情報を扱っていても、安全管理措置が異なる場合がある
- そのため責任分界を契約で明確にしておくことが重要である。
- 関係者間の連絡体制や問題発生時の対応体制を明確にしておくことも重要である
- 厚生労働省から公開されている「医療情報システムの安全管理に関するガイドライン　４章　電子的な医療情報を扱う際の責任のあり方」を参考にすること

（３）要員の交代や変更が多い点
- 地域見守りサービス及び地域見守り支援システムには複数の要員が関わっており、日によって担当者が変わるような運用が想定される
- 予定していない急な要員の交代等も日常的に起きるであろう
- その場合の利用者認証やアクセス制御といった技術的対策と、運用管理規程の実施の徹底のための教育といった運用的対策について十分に検討し、セキュリティ対策に不備が出ないようにすること

（４）秘匿性と可用性のバランスが重要な点
- 地域見守りサービスは個人情報保護法に準拠し、確実に個人情報を保護することが必要であり、そのため確実に利用者認証とアクセス制御を行わなくてはならない。
- ただし、サービスの性格上、アクセス権限がない利用者が臨時にアクセスしなければならないケースがあり得ると考えられる。
- そのような場合の非常時のアクセス手法について運用規定に盛り込んでおくべきである。
- 例えば「ブレークグラス」という手法は、非常時の使用に備えたユーザアカウントを用意する手法である。ブレークグラスでは非常時用ユーザアカウントは通常時の明示的な封印、使用状態に入ったことの周知、使用の痕跡を残すこと、定常状態に戻った後は新しい非常時ユーザアカウントへ変更をすることを基本としている。

（５）利用者のITリテラシーが多様な点
- 医療機関単一で運用している場合は、ある程度のITリテラシーの確保は図れる
- 地域見守りサービスでは様々な職種の方々が係わるため、ITリテラシーの差が非常に大きくなると想定される

・ そのことも想定したセキュリティ管理が必要である
・ 例えばITリテラシー底上げのための教育は重要である

（６）救急対応時の情報提供等を考慮する点
・ 救急時の情報提供が地域見守りサービス及び地域見守り支援システムの目的に含まれており、そのケースの運用規定が定められている場合は問題ない
・ そうでない場合、救急時に支援システムから情報を提供することは第三者提供の扱いとなるため注意が必要である
・ 第三者提供の扱いについては、個人情報保護法では本人同意が必要との制限がかかっている。
・ ただし、「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」は例外として本人同意を必要としていない。
・ どのような状況ならばこの例外が適用されるのかを慎重に検討しておくこと

（７）真正性の担保が必要な情報を扱う可能性がある点
・ 法律や規制により、扱っている情報の真正性の担保が求められる場合は、監査対応のために、確定操作手順や改訂履歴の保存が求められる
・ 扱っている情報を抽出し、それに対する法律や規制の要求事項を洗い出し、真正性の担保が求められている情報かどうかを確認すること
・ もし、技術的に担保できなければ運用で担保できるように運用規定を定めること

（８）情報を扱う場所、機器の種類が多様な点
・ 情報の保存は管理された場所に設置されたサーバで行うと想定されるが、ネットワークを通じてその情報にアクセスする端末が存在する場所については様々なケースが想定される
・ 見守り対象者や関係者の家から、移動中の車中から等がありうる
・ また、利用するネットワークについても、専用線、IP-VPN、インターネット等の種別がある
・ 機器についても、デスクトップ型、ノート型ＰＣ、ＰＤＡ、携帯電話等があるであろう
・ 利用する場所やネットワークに応じたセキュリティ対策が必要である

６．２　セキュリティ管理における用語および一般的な要件

セキュリティ管理業務については、情報セキュリティ(機密性、完全性、安全性) を

確保することを目的とし、主に以下の要件を満たすようにシステムを運用管理する。

（1）基本的な概念

	項目	内容	要件
1	機密性	認可されていない個人、エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性。	個人情報保護の観点では、アクセス者は、利用目的と情報主体に対してその個人の同意が必要。
2	完全性	資産の正確さおよび完全さを保護する特性。	入力した情報と出力した情報が、食い違っていないこと。
3	可用性	許可されたエンティティが要求したときにアクセスおよび使用が可能である特性。	許可されており必要な時に情報にアクセスできること。 診療録の電子保存３基準では、見読性、保存性に分かれている。
4	真正性	ある主体または資源が、主張どおりであることを確実にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。	改ざん、書き換えなどがなされていないこと。
5	責任追跡性	あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できることを確実にする特性。	セキュリティ侵害の検知と、事後調査を可能にすること。
6	信頼性	意図した動作および結果に一致する特性。	要求された機能で動作すること。
7	否認防止	ある活動または事象が起きたことを、後になって否認されないように証明する能力。	ユーザの利用を事後になって否認されることを防止すること。

（2）情報セキュリティのリスク

	項目	内容
1	情報資産	情報セキュリティにおいて守るべき対象のこと
2	脅威	情報の機密性・完全性・可用性を阻害する要因
3	リスク	脅威によって情報資産が損なわれる可能性
4	インシデント	実際に、情報資源が損なわれてしまった状態
5	脆弱性	一つ以上の脅威がつけ込むことのできる情報資産がもつ弱点

（3）　情報セキュリティの確保

	項目	対策
1	機密性 （漏洩防止）	情報システム間での通信の機密性の確保、 情報システム単体に対する機密性の確保など
2	完全性 （改ざん防止と検出）	ハッシュ値とメッセージダイジェスト（要約情報）など
3	可用性 （システムダウン防止、アクセス不能防止）	電源の冗長化、サーバやルータ、ネットワークの冗長化や負荷分散、ネットワークのセグメント化など
4	真正性	電子署名、タイムスタンプなど
5	責任追跡性	アクセスログ、監査ログなど
6	信頼性	仕様の明確化、ソフトウェアの品質保証など
7	否認防止	認定特定認証事業者等の発行する電子証明書を用いて電子署名を施す。 電子署名を含む文書全体にタイムスタンプを付与する。 上記タイムスタンプを付与する時点で有効な電子証明書を用いる。

６．３　ネットワーク上のセキュリティの確保

見守り支援システムを提供する上では、多様な職種や地域に分散する各施設間の連携などが重要になる。これをネットワーク上で実現する際には、下記の通り技術的な対策と運用面での対策を検討することで、責任の分解点を明確化し、管理責任の重複と空白を作らないことが重要である。

	項目	対策
	技術的な対策	
1	チャネルセキュリティ	通信の起点・終点識別の認証となりすましの対策（相互認証）として、IPSec+IKEで実行すること。
2	オブジェクトセキュリティ	盗聴への対策として暗号化、改ざんへの対策として電子署名（HPKI）＋タイムスタンプを施すこと。
3	相互認証	資格確認には、HPKIで医療資格者と保健医療機関の認証用電子証明書発行の仕組みを定めている。
	運用的対策 （責任分界点を明確化して、管理責任の重複と空白をつくらないこと）	
4	情報の通信側・受信側の責任分界点	送信側はどの時点が責任範囲か、受信側はどの時点から責任が発生するかを明確にする。

5	通信を形成する事業者の責任分界点	ネットワークを経由する情報伝送では、送信側・受信側のどちらでもない事業者の管理運営する経路を通過するのが普通である。中間の回線事業者、ネットワークサービス提供者を含めた関係事業者間で、管理責任範囲を明確にし、事故発生時の一義的な対応者を定めておくことが求められている。

7．情報管理

7．1　医療に係わる諸記録

見守り支援システムに関係してくるであろう医療機関に備えられている記録は、医療法第 21 条に「医療に係わる諸記録」が定められている。

	項目	記録	備考
1	診療に関する諸記録（すべての病院が備えるべき記録）	病院日誌	
		各科診療日誌	
		処方せん	
		手術記録	
		看護記録	
		検査所見記録	
		エックス線写真	
		入院患者及び外来患者の数を明らかにする帳簿	
		入院診療計画書	
2	（特定の病院が備えるべき記録）	紹介状	
		退院した患者に係る入院期間中の診療経過の要約（退院時サマリ）	

7．2　情報の発生源別分類

見守り支援システムの周りで扱われる情報の発生源は、さまざまである。どのような情報がどのような目的で記録・保存され、それらを必要なときにどのように活用できるのかなど、今後さらなる議論が必要である。

本年度は、これらの情報発生源を特定し、セキュリティ上のリスクマネジメントの観点から、見守り支援システムで扱う可能性のある情報資源を明確にし、それらの管理に対するリスクアセスメントを試みた（附属書 B および C 参照）。

7．3　医療情報管理の考え方

医療は、医師だけでなく看護師、薬剤師、検査技師をはじめ、栄養管理士、理学療法士、作業療法士、言語聴覚療法士などの多くの医療者が協同して行うことが不可欠

である。そこで、医療記録は、一連の記録として参照できるように管理されるべきである。

特に、介護医療の分野では、介護福祉士、社会福祉士などが患者および家族の生活面の支援に当たる社会福祉系の専門職（MSW）、心理的支援にあたる心理学専門職などが、対象者（本人、家族）との間に介在する。さらに、本人も積極的に医療の内容を知ることがよい効果を生み出すとされている。

（1）継続性および概括性の保証

具体的には、到達目標に即した実行計画を明示して、多職種による医療行為の相互関係が分かるように記録し、継続して行った医療プロセスが情報分析、参照の際に、鳥瞰できるように構造化して保存する必要がある。

一般的な患者情報の処理過程（診療プロセス）は、以下の通りである。

	項目	内容
1	情報取得	患者、家族などから愁訴、診察、検査などの情報を取得
2	評価の集約	多職種にまたがる複数の医療者による多角的な分析、推論、考察
3	計画立案、選択	追加の検査、治療法、看護法の計画
4	医療の実施	処置、治療、教育指導
5	成果情報の取得	処置治療後の患者の反応、治療効果情報など
6	総合評価	診療・看護組織、過程および結果の総合評価

（2）真正性の保証

医療記録は、社会的に証拠能力をもつ公文書であり、医師法で、遅滞なく記録することが規定されている。専門職が分業する医療チームでは、最新のデータ、事実に基づき客観的に記載し、すみやかに情報共有することが必要である。真正性を保証するには、以下のことを考慮すること。

	項目	内容
1	観察記録	客観的に記述し、最新のデータを提供する 特に、推論、推測部分は、そのことが明確になるように表現する
2	指示記録	指示、指示受け、実施前確認を系統的に記載する
3	時刻の整合性	複数（多職種）で記録する場合に、時刻の不一致は許されない
4	口頭指示	緊急時をのぞいて、原則、口頭だけの指示は行わない その場合は、事後記録として明示する
5	訂正	電子記録では、上書き、削除できにないようにする 誤記などのないように誤りが生じた場合は、原則、訂正日時、訂正者名を明記し、訂正内容がわかる形で記録する
6	著名	責任性を担保するためエピソードごとに記載する 電子記録の場合は、電子署名をつける

７．４　アクセス管理

情報（ドキュメントなど）の種別ごとに、役割（職種、職位、資格などを含むロール）に基づきアクセス権限を行う必要がある。具体的には、アクセスが許される情報種別ごとに利用者の役割を規定するアクセス制御マトリックスを決定し、システムのアクセス制御機能を用いて動的に、かつ適切にアクセス制御がなされるべきである（要求定義書暫定版附属書Ａ．１０節　表Ａ．１０－１参照）。アクセス制御の単位は実装によっては、データ、レコード、ファイル、あるいはフォルダ（ディレクトリ）、データベースなど、さらに細かい単位でアクセス制御が必要になる場合もある。

７．５　ライフサイクル管理

医療サービスおよび介護サービスにおいては関係する各種法令により保存期間が定められているものがある。医療サービスにおいては医療法、医師法に定められる診療録等の５年間の保存期間、あるいは介護サービスの提供に関する諸記録については介護保険法により２年間、またその他地方自治法を配慮した場合の５年間の保存期間、要介護認定資料等の原本保存の期間５年間など見守り支援に関連する文章の保存期間はまちまちに設定されている。

これら関係法規を鑑みた保存期間のポリシーを策定し、ライフサイクルマネージメントを適切に実施する必要がある。

見守り対象者にとって、提供されるサービスに満足が得られない場合、サービスの事業者を変更することもあり得る。逆に、途中で事業者側がサービス契約を打ち切ったり、事業体を解散せざるを得なかったりする場合もある。このような場合、他の事業者に適切に引き継がれたりする必要がある。

また、上記の他、死亡等にともない見守り対象者のデータは適切な期間保存し、必要に応じて破棄などの処置がされなければならない。

８．システム管理業務

システム管理業務は、地域見守りシステムを運用する上で必要となるシステムの安定性および安全性を維持することが目的である。特に、障害が発生しても、速やかに対処し「復旧」することが求められる。管理すべき対象は、ハードウェア、ソフトウェア、データ、ネットワークなどだけではなく、分散する利用者及び利用者の施設の設備などにも及ぶ。

地域見守りシステムのシステム管理の主な業務は、以下のとおりである。

･組織・利用者管理
･システム維持管理
･システム監視
･バックアップ
･障害時対応

８．１　組織・利用者管理

システム運用者は、施設の登録申請書による施設の登録、更新、削除、及び利用申請書による利用者の追加、削除、変更の依頼があった場合、以下の業務を実施する。

	業務	内容
1	施設の登録、更新、削除	システムの運営組織から、システム運用者への書面による依頼により、施設、事業者を登録、更新、削除を行う。
2	利用者の登録	利用者の追加に際しては、利用者ID 及び暗証番号のコード要件に適合するユーザID 及び暗証番号を決定･登録する。そのユーザID･暗証番号、別に定める利用の手引きを申請責任者に封書で知らせるものとする。
2	利用者の削除	利用者の削除に際しては、その要求に対して速やかに削除するものとする。
3	利用者の変更	利用者の変更に際しては、上記1と2の処理を行うものとする。
4	本人確認	利用者に関する付随情報については、当該利用者の本人確認を確実に実施した上で要求に応じて変更するものとする。

８．２　システム維持管理

システム管理者は、受け入れたシステムのハードウェア及びソフトウェアに対する以下の維持管理を実施する。

	業務	内容
1	システム構成管理	システムを構成するハードウェア、ソフトウェアに関して、以

		下の内容を正確に把握して記録、管理する。 ・機器特定情報（機器管理番号、機器名称、型式、製造メーカ、製造日） ・導入形態（契約区分、導入日、更新予定日） ・経費情報（購入価格、リース月額、保守費） ・ネットワーク接続情報（IPアドレス、接続ポート、接続ポート番号） ・導入ソフトウェア（ソフトウェア名称、バージョン） ・利用者端末、サービス配置の登録管理
2	ハードウェア、ソフトウェアの維持管理	・ハードウェアに対しては、メーカの指示に従い、定期的なリブートなどの維持管理を行い、操作履歴を記録する。 ・ソフトウェアに対しては、メーカ等からの指示に従い、バグ対応やセキュリティホール対応などの維持管理を行い、履歴を記録する。 ・ソフトウェアの維持管理を実施した時は、システムファイルのバックアップを確保する。
3	クライアント側の更新管理	・サーバ側のプログラム変更後、必要ならクライアント側のアプリケーションの更新を行う。次の２つの方式がある。 ①プル型更新 更新情報を通知されたのち、随時、利用者側で更新の操作を行う。 ②プッシュ型更新 クライアント側のPCを立ち上げたとき、または定時に、自動更新する。
4	システムの停止を要するメンテナンス時の体制	・大きなシステムの修正を行う場合、または緊急性の高い修正が必要なときは、夜間などサービスを停止して、システム管理者が手動で更新を行う。 ・システムの受け入れ(インストール、更新) システムの開発･構築･改修後、システムデータについては、受け入れ時及び変更時にバックアップを取り、1 年間保管するものとする。

８．３　システム監視業務

監視業務は、各サーバの障害を検出することを目的とする。

システム管理者は、受け入れたシステムの運転操作(起動停止など) 及びシステムの稼働監視を以下により実施する。

	業務	内容
1	自動/手動運転	システムの運転操作は自動運転とし、データの削除処理及びシステムの異常等によりシステム停止を要する時のみ、手動運転操作とする。
2	生死監視	システムの稼働監視は、Pingによる5 分毎の生死監視、15 分毎のシステムアプリケーションの応答監視、さらにファイヤー･ウォールのアクセス･ログを定期的にチェックする。

3	不正アクセス監視	アクセスログを定期的に監視し、不正アクセスに対処できるようにする。
4	運転手順書の常備	上記に必要な運転手順書はシステム管理者がいつでも参照できるよう常備するものとする。

８．４　バックアップ業務

８．４．１　バックアップ方式

レジストリおよびリポジトリのバックアップは、各システムにて自動、または手動で実施する。

バックアップには、日々行う日次の業務データのバックアップ、メンテナンス時や設定変更時など不定期的に取得する保守時バックアップがある。

	方式	内容
1	差分バックアップ方式	前回バックアップ時点からの更新分データのみを取得することでバックアップ時間を短縮させる方式
2	フルバックアップ方式	全データのバックアップを毎回取得する方式(取得時間は長いがバックアップからの復旧手順が単純)
3	オフラインバックアップ	システム停止中にバックアップを取得する方法のため、業務運用が一時的に使用不可となる
4	オンラインバックアップ	システム稼動中にバックアップを取得する方法のため、業務運用の24時間稼動が可能となる

通常は、日次の差分オンラインバックアップを行い。週次のフルオンラインバックアップを実施する。

システム構成の変更などの保守時には、オフラインのフルバックアップを行う。

８．４．２　データ･バックアップ

システム管理者は、システム内にて対象者の同意を得た上で一時保管している利用者の複製診療情報について以下のデータ･バックアップ処理を行うものとする。

	項目	内容
1	自動データ・バックアップ（毎日/毎月）	利用者が他施設へデータを発信した日から起算し、少なくともX年間の保管に万全を期すために、毎日及び毎月定められた日時に自動データ･バックアップ処理を行う。
2	責任者の承認	自動データ･バックアップ作業を行う日時については、あらかじめ責任者の承認を受けるものとする。
3	日時を利用者に公開	管理組織からの承認後、毎日及び毎月のデータ･バックアップの日時を、管理組織サイトにより予め利用者に公開するものとする。

4	サービスの停止	毎月１回のデータ･バックアップ作業時については、提供するすべて又はその一部のサービスを停止することができるものとする。また、システム停止を伴う作業が発生する場合は、その内容を予め管理組織サイトにより利用者に公開・通知するものとする。
5	データ削除	利用者が他施設へ発信したデータについては、発信日から起算してX年間経過後、削除するものとする。ただし、医学研究への参加に同意していただいたデータは除く。
6	データ保管	上記５のデータの削除以降、利用者のやむをえない事由による申し出により、データの臨時使用に対応することを目的に、上記１の自動データ･バックアップとは別に、上記５で削除するデータを外部保管できる媒体にバックアップを行う。 バックアップされたデータは、機密保持に万全を期して管理、保管するものとする。
7	保管の期間	上記６で外部保管できる媒体にバックアップしたものは、外部保管時点から起算してX年間保管するものとする。

８．４．３　バックアップツールによる管理例

バックアップは、ツールを利用して、テープなどの可搬媒体にバックアップする。ツールの利用の流れ（例）は、以下のとおりである。

	操作・機能	内容
1	クライアントの登録	･クライアント（対象）を追加する ･管理単位を設定する ･クライアントのグループを登録する
2	バックアップ装置の登録	･バックアップ装置（テープなど）を認識させ、追加登録する ･共有装置を設定する
3	バックアップ装置の管理	･バックアップ装置のライブラリ、ドライブを選択する ･コンフィグレーション･オプションを設定する ･メディアにラベルをつける ･ブランク処理をする ･再利用のマークをつける
4	バックアップの管理	･サーバを選択する ･スケジュール（実施間隔）を指定する ･対象の選択（バックアップ装置、メディアなど）する ･オプションを指定（圧縮、検証、複製など）する ･データベースの管理を行う
5	リストアの管理	･サーバを選択する。 ･対象を選択（クライアント、フィルタ）する ･スケジュールを指定する ･オプションを指定（解凍、リストアタイプなど）する ･データベースの管理を行う
6	ステータスの監視	･サーバを選択する。 ･装置のステータスを表示する

		･ジョブステータスを表示（スケジュール済み、実行中、完了）する ･情報メッセージをみる
7	その他の管理	･ログファイルを管理する ･ジョブ実行、履歴のレポートを見る ･ポリシーを設定、管理する ･アクセス制御を行う ･グローバル通知で、管理者に知らせる

８．５　障害時の対応業務

８．５．１　障害対策の体制

システム管理者は、システム管理業務の中で発見したシステムの異常、システム運用者から不具合の連絡を受けた場合、以下の事項を実施し、その内容を記録するものとする。

		対応
1	状況確認	システムの異常または不具合の状況を確認する。
2	分析・復旧	原因を分析し、その復旧のため関係箇所(メーカ、ベンダー、システム構築箇所など) と連係し、早期復旧に努める。
3	状況報告	利用者等の利用に影響が及ぶ場合は、状況に応じて管理者のウェブサイトへの掲載、及びあらかじめ定めた連絡先に電話･FAX･e-mail 等により状況、復旧予定などを報告する。
4	課題報告	システム管理業務の一環で対応できない再発防止策が必要と思われる場合は、その内容を整理し、運用責任者に報告する。
5	対策検討	それらを受け運用責任者は必要に応じて臨時の実務委員会を召集し、事故防止の対策を検討した後、総会で計る。

	段階	作業	内容
1	発生/判断/連絡	障害の把握	･サーバのメッセージ、各施設からの電話連絡内容より、障害状況を把握する。
		障害運用方法の決定	･障害区分の切り分け、影響、時間などから対策方法を決定する。
		連絡	･障害内容により､システムに関連する各機関に電話連絡する。 ･担当施設全体など､障害区分により連絡範囲と連絡手段を決めて連絡する。
		指揮	･障害時に指揮者として機能する。
2	障害時運用	該当施設の障害時運用支援	･障害時運用の指導、資料の提供など。

		復旧	･システムダウンの場合、一刻も早く立上げ、復旧に努める。
		原因追求	障害原因の特定と対策をとる。
3	復旧／後処理	復旧確認	･サーバ コマンド等を投入し、正常動作していることを確認する。 ･クライアント 端末が正常動作していることを確認する。 業務アプリケーションが正常動作していることを確認する。
		復旧の連絡	･決められた手順で、復旧の連絡をとる。
		後処理	データの後追い入力、ファイルの回復方針を検討し、推進する。

８．５．２　障害防止および発生時の対策

（1）障害防止

･保守／予防保全

障害の予防保全、保守活動を日常実施する。

･再発防止

万一障害の発生したときは、復旧後に再発防止策を検討し、実施する。

（2）障害発生時の対策

障害発生時の作業の流れは、以下のとおり。

８．５．３　障害時の運用

サーバ、クライアントおよび周辺装置のハードウェアならびにソフトウェア等に障害が発生した際には、以下のとおり効率良く対処する。

	対応	説明
1	障害連絡ルート	システムの障害発生時の連絡、復旧通知、対応等を混乱なく効率良く行うために、関連する施設、部署において障害連絡ルートを定める。
2	有人運転時間帯の障害対応	有人運転時間帯に障害が発生した場合、業務に与える影響が多大なため、速やかに回復作業を実施すると共に、「障害連絡ルート」に従いシステム管理者は関連施設、部署に連絡する。 原則システム再開後のサービスの再起動は、センターのシステム保守部署の判断に従う。システム保守部署との連絡が取れずサービスの再起動判断ができない場合は、サービスを起動しない。 障害による影響がオンライン業務に直ちに影響を与えない場合は、極力オンライン業務の継続を優先させ、回復作業については夜間バッチ等を含め影響度合いを考慮して時期および範囲を決定する。な

		お、各施設のシステム保守部署との調整によりオンライン時間を短縮し、リカバリ作業を実施する場合がある。
3	無人運転時間帯の障害対応	無人運転時間帯にシステムに重大な障害が発生した場合は、翌X:XX以降にサーバ監視者により、連絡ルートを経由してシステム管理者に連絡が行われる。システム管理者は、障害内容を確認し、必要に応じ各システム担当者に連絡する。 又、無人時間帯に現場より障害連絡を受けた場合は、システム管理者は関連部署へ連絡を行うが、障害対応は翌X:XX以降となる。
4	障害連絡	システムダウン時には、システム管理者は以下の連絡を行う。 ･システムダウン発生連絡 ･システムダウンの発生または､システムダウンと同様の状態となった場合、システム管理者は各施設のシステム保守部署及び関連部署に対して障害発生連絡（第一報）を行う。
5	影響範囲･リカバリ終了予定連絡	影響範囲の調査と並行し、各システム保守部署と連絡の上、リカバリ予定時間を設定し、終了予定時間を各施設のシステム保守部署及び関連部署に対して行う。 また、代替運用可能な場合は、運用切り替え(伝票運用など)の電話連絡･院内放送などを行う。
6	リカバリ終了連絡	業務リカバリが終了した段階でオンライン処理などを起動する。また、正常動作を確認した段階で、リカバリ終了報告を各システム保守部署及び関連部署に対して行う。
7	設備系障害	設備系障害としては、ネットワーク系障害、電源障害、空調障害、大規模災害などが挙げられる。 各障害における「システムの動作」、「業務への影響」、「対処方法」は以下のとおりとなる。 （対処方法） システム管理者は、各設備担当部署からの復旧連絡後、各システム担当部署へ連絡を行う。連絡を受けたシステム担当者は、中断された業務処理の有無など各システムの整合性を確認し、必要に応じてデータの修復および業務処理の再実行後、各システムのサービスを開始する。

８．５．４　障害別対応策

通常、障害の発生直後は現場が混乱し、原因究明までには長時間かかることがほとんどである。このようなとき、まず第一に現象からおおよその原因を推測し、障害の発生から原因の究明および、回復までに短期間（1時間以内）で対応できるかを判断する。

そのためには、障害の各パターンをよく認識しておき、部分障害か全面障害か、回復見通しなどを判断する必要がある。

また、判断のための情報（各施設、部署の適用状況など）は積極的に収集し、正確な情報を得ることが大切である。各施設、施設内の役割分担を決め、各担当者が臨機応変に対処できるようにする。

以下に、典型的な障害の種類と、その対応を定める。

（1）ハードウェア障害（例）

	種別	対応	内容
1	電源障害	現象	･停電のため、各ハードウェアが停止した。 ･瞬停のため、各ハードウェアが停止した。
		推定原因	･停電 ･落雷
		対応策	･手順に従い、再立上げ。 ･機器によっては無停電電源装置により、処理継続。
		復旧見通し	回復後、即時
2	CPU、メモリ障害	現象	･画面表示が静止状態となり、コマンド入力ができない。 ･サーバプログラムの停止により、すべての業務が行えない等。
		推定原因	CPU内の基板障害などによる、致命的な障害
		対応策	･全面手作業で運用。 ･サーバマニュアルにてシステムメッセージを参照し、必要な操作を確認。 ･CPUの状態を確認。
		復旧見通し	通常、縮退運転が可能のため、システムダウンは回避できる。
		防止策	サーバのマニュアルを参照。
3	ディスク障害	現象	画面にエラーメッセージが表示される。
		推定原因	･不当トラック発生によるI/Oエラー ･ディスクのアーム障害などによる、致命的な障害
		対応策	･システムメッセージを参照し､オペレータの操作を確認。 ･ディスク駆動装置のマニュアルを参照。
		復旧見通し	通常､RAID10 のミラーリングのため､システムダウンは、回避できる。
		防止策	定期点検を行い、予防を推進。
4	LAN 障害	現象	･クライアント端末のネットワークで、他のマシンを見ることが出来ない。 ･システムにて情報が、送受信出来ない。 ･画面にエラーメッセージが表示される。
		推定原因	･LANケーブルが正しく差し込まれていない。断線している。 ･HUBの障害 ･LAN ボードの障害
		対応策	･障害箇所を特定し、障害の起こっている場所を探し、障害内容により対応する。 ･PING コマンド等投入し障害状況を特定し、保守員に連

			絡する。
		復旧見通し	必要な時間の目安を、別途定める。
		防止策	定期点検を行い、予防を推進。
5	ルータ障害	現象	･パネルに異常なステータスコードが表示される。（正常時は何も表示されない） ･一部の施設、部署でしか業務が操作不可。他施設の情報の参照不可。
		推定原因	･ルータの電源がOFFになっている（無停電電源装置がない場合）。 ･ルータ内部の致命的な障害 ･ポート部分の接触不良障害
		対応策	･ルータの電源を入れる。 ･ステータスコードを確認し、PINGコマンド等投入し障害状況を特定し、保守員に連絡する。 ･ルータのハードウェアマニュアルを参照。
		復旧見通し	必要な時間の目安を、別途定める。
		防止策	定期点検を行い、予防を推進。
6	クライアント障害	現象	･端末が起動できない。 ･マウスのポインタが動かない。 ･キーボード入力が出来ない。 ･画面の表示が乱れる。 ･次の画面が展開されない。
		推定原因	接続機器（マウス、キーボード等）が正しく接続されていない。 ･立上時の電源投入順序誤り ･クライアントの各設定不良 ･立上時にシステムディスク以外の装置がセットされている。 ･クライアント内部の致命的な障害（ハードディスク、CPU） ･液晶画面のTFT障害
		対応策	･クライアントへの接続機器が正しく接続されていること、電源が入っていることを確認し、再立上げを行う。 ･クライアントの交換をする場合、決められた手順で端末を設定する。 状況を確認し、保守員に連絡。
		復旧見通し	体制などを考慮して必要な時間の目安を、別途定める。
		防止策	･クライアントのハードウェアマニュアルを参照。 ･クライアントの設定を変えないように指導。 ･予備機を準備し、端末設定手順を把握。

（2）ソフトウェア障害

	種別	対応	内容
1	DB障害	現象	･DBが起動しない ･DBがマウントされない
		推定原因	･容量不足 ･ファイル破損
		対応策	･障害時運用に切替える。 ･マニュアルを参照し、障害回復作業を行う。
		復旧見通し	体制などを考慮して必要な時間の目安を、別途定める。
		防止策	･環境設定が正しいことを確認。 ･決められた手順で運用。
2	レスポンス低下	現象	･端末とサーバとの通信に通常より時間がかかる。 ･利用者からクレームの電話がある。
		推定原因	･サーバのCPU使用率増大。 ･サーバ又はクライアントのメモリーリーク ･業務ファイルにおけるファイルのI/O時間が大になったため。 ･プログラムのループ
		対応策	･CPUのI/Oで使用率の高いジョブ／ファイルを調査。 ･トランザクション稼動状態（プログラムのループ）を調査。 ･障害メッセージの表示有無を画面又はログより検索。
		復旧見通し	障害メッセージがある場合は、その対策に従う。
		防止策	･ファイル又はDBの再編成を行う。 ･プログラムの見直しを検討する。
3	OS障害	現象	OSの異常終了
		推定原因	･環境ファイル破壊 ･OSの設定不良
		対応策	･環境設定ファイルが正しく設定されていることを確認。 ･全面手作業で運用。
		復旧見通し	体制などを考慮して必要な時間の目安を、別途定める。
		防止策	･環境設定が正しいことを確認。 ･決められた手順で運用。
4	クライアントでのソフトウェア障害	現象	･端末のエラーメッセージが表示される。 ･端末の異常終了 ･端末の画面表示及び展開がされない
		推定原因	･クライアントのハードウェア障害 ･OSの設定不良 ･OSの領域破壊 ･ドライバの破損（プリンタ･LAN等） ･環境ファイル破壊

		対応策	･クライアントに添付されているマニュアルを参照し、エラー内容を調査。 ･内容により、再システムセットアップを行う。
		復旧見通し	体制などを考慮して必要な時間の目安を、別途定める。
		防止策	環境設定が正しいことを確認。

９．セキュリティ管理

一般的にセキュリティ対策とは、情報、ハードウェア、ソフトウェアなどの資産を安全に保つための個々の対策のことである。例えば、情報漏洩を防ぐための利用者認証、コンピュータウイルス対策、データのバックアップなどのことである。

地域見守りサービス及び地域見守り支援システムでは、見守り対象者への適切なサービスを行うため、その人の個人情報および医療情報を取り扱うことが想定される。医療情報は個人にとって最も機微な情報であり、それを取り扱う事業者に対しては、取り扱いに特段の注意を払うことが法律上求められている。そのために適切なセキュリティ対策を実施することは必要不可欠の要件である。

さらに、誤りのないサービスを提供するための情報の完全性の維持や、有効なサービス提供のための可用性の維持、例えばシステムやネットワークの安定稼働・性能維持、トラブル発生時の迅速な復旧対応なども求められる。これらもセキュリティ対策に含まれる。

これらのセキュリティ対策は、予め策定された基本方針に基づき、守るべき対象と、それらに対する脅威を明確にした上で、リスクアセスメントのなかで決定されるものである。そして、対策が確実に実行されていることが確認され、適宜改善されていかなくてはならない。また、以上のようなリスクアセスメントの結果や改善状況については文書として保管し、必要があれば第三者へ説明のため開示できるようにしておかなくてはいけない。セキュリティ管理とはそのような体制を構築することである。

セキュリティ管理を適切に行っていくことで、見守り対象者をはじめとする関係者からの信頼を確保するとともに十分にバランスのとれた情報セキュリティを構築し、維持していくことにつながる。

セキュリティ対策は、どちらかといえば、完璧に資産を脅威から守ることに重点が置かれるが、セキュリティ管理はそれだけでなく問題が発生した場合に的確に対処できるようにしておくことなども含まれている。

もし、セキュリティ管理を行わなかった場合、以下のような不都合が発生する恐れがある。

（１）不適切なセキュリティ対策の適用

- 例えば、資産の価値に比較してコストの高い対策を実施、
- 発生頻度が非常に低い脅威に対し発生頻度が高いものと同様の対策を実施、
- 対策が漏れた部分から情報の漏洩など問題が発生、

・ 運用に対し不適当な対策を実施したために業務に支障が発生するなど。

（2）セキュリティ対策の未実施

・ 従業者に対して対策の周知徹底が図られず、適切に運用されない
・ 実施状況の確認が行われず、計画された対策が実際には行われていない状況が発生する。

（3）セキュリティ対策の陳腐化

・ 実施状況の見直しを行わないために、技術的に陳腐化したり、問題が見つかった対策を継続して利用してしまう

（4）問題発生時の対応の遅れ

・ 問題が発生した時の対応手順が明確でなく復旧に時間がかかる
・ 利用者からの苦情処理対応手順が立てられておらず処置が迅速に行えない

9．1　セキュリティ管理の概要

セキュリティ管理は、以下のステップを繰り返し実行することで実施される。

・ 基本方針の策定と、それに基づいた具体的な計画の策定
・ 計画の実施
・ 実施状況の定期的な評価
・ 必要に応じて計画の見直し

これらのステップの繰り返しは、1）計画(Plan）、2）実施(Do）、3）評価(Check)、4）見直し(Act)といういわゆるPDCAサイクルを実施することである。PDCAサイクルは事業活動における生産管理や品質管理などの管理業務を円滑に進める手法の一つであり、セキュリティ管理においても非常に役立つものである。「医療情報システムの安全管理に関するガイドライン」でも推奨されている。

本項以降で、それぞれのステップで行うべき内容について説明する。

9．2　計画の策定

セキュリティ管理では計画の策定が最も重要である。以下のステップで行う。

（1）フェーズ1

①適用範囲および境界を定義
②基本方針を定義

（2）フェーズ2

③リスクアセスメントの取組方法の定義

④リスクを特定
⑤リスクを分析し評価
⑥リスク対応
⑦管理目的と管理策を選択

（3）フェーズ3
⑧残留リスクの承認
⑨導入・運用の許可
⑩適用宣言書作成

９．２．１　フェーズ１
セキュリティ管理の適用範囲と境界を明確に定義し、基本方針を策定する。なお、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」において、個人情報保護に関する基本方針を定め対外的に公開することが求められている。

以下の点を考慮して適用範囲及び境界を定義する。
事業内容
体制
所在地
資産
技術の特徴

セキュリティ管理の目的や目標は、事業内容や体制によって異なり、要求事項も社会的な要求（法令、業界の慣習、顧客満足など）、内部的な要求（事業継続、内部統制）の双方があり、これらから適用範囲を定義する。
適用範囲の定義の内容により、今後実施するセキュリティ管理体制の作業負荷が大きく影響されるので十分検討を行って決定すること。

基本方針とは法の順守と個人情報保護への積極的な取組について組織としての対応を宣言するものである。個人情報を扱うシステムの安全管理についてもその中で言及すること。基本方針は、その後に行うリスクアセスメントやセキュリティ管理の実施や評価、改善の元となる文書である。

セキュリティ基本方針に含まれる内容は以下のとおりである。
1）適用範囲
2）目的

３）個人情報保護の理念、法の順守
４）情報の取り扱いや保存方法と期間
５）セキュリティ管理への対応
６）苦情及び相談への対応
７）代表者の氏名

詳細は「附属書Ａ　５．１．１　情報セキュリティ基本方針文書」を参照のこと。

９．２．２　フェーズ２

本フェーズでは、資産の洗い出し、資産に対する脅威の洗い出し、リスクアセスメント、対策の選択などを行っていく。

詳細は「附属書Ｂ　情報資産の明確化」および「附属書Ｃ　リスクアセスメント」を参照のこと。

９．２．３　フェーズ３

本フェーズでは、フェーズ２でリスク対策を行った後に残っているリスク（残留リスク）の検討、承認を行い、組織全体としてセキュリティ管理に関しての運用内容の導入の承認を行う。

そして最後に選択した管理目的と管理策の内容と、それを選択した理由を記述した適用宣言書を作成する。これには管理策を適用除外したものに対しても、適用除外した理由を記述する。

９．３　計画の実施

９．２節で策定した計画に基づき対策を実施する。以下の手順で行う。

１）実施計画の策定
２）資源（人、資金）の割り当て
３）計画の実施
４）有効性の測定
５）教育、訓練
６）運用状況の管理やセキュリティインシデントへの対応

９．４　評価

実施状況が計画通りか、計画で想定した効果が出ているかを定期的に評価する。システムの構成が変更された際にも評価が必要である。以下の手順で行う。

１）評価のための手順の策定
２）評価の実施

3）評価結果のレビュー
4）計画の更新

9．5　改善

9．4節での結果を基に、計画の改善を行う。以下の手順で行う。

1）改善策の実施
2）変更内容の通知

１０．在宅機器の管理

管理対象機器と管理項目の詳細については次年度の課題とする。

（1）在宅機器

在宅で使用する医療機器、医療衛生材料、見守り機器には、以下のものがある。

	項目	在宅機器・材料
1	福祉用具	（福祉用具貸与の対象品目） 車いす、車いす付属品、特殊寝台、特殊寝台付属品、床ずれ防止用具、体位変換器、手すり、スロープ、歩行器、歩行補助杖、認知症老人徘徊感知機器、移動用リフト
		（介護予防福祉用具貸与の対象品目） 手すり、スロープ、歩行器、歩行補助杖
		（特定福祉用具購入費の対象品目） 腰掛便座、特殊尿器、入浴補助用具、簡易浴槽、移動用リフトのつり具の部分
		（居宅介護住宅改修費の対象） 手すりの取り付け、段差の解消、滑りの防止、移動の円滑化のための床材の変更、引き戸等への扉の取替え、洋式便器の取替え、その他
2	医療機器	喀痰吸引器、ネブライザー、パルスオキシメーター、酸素濃縮装置、点滴台、心電モニター、血糖測定器、車椅子、その他
3	医療衛生材料	ガーザ・綿球、胃チューブ各種、経管栄養セット、留置バルンカテ各種、導尿バック、吸引カテーテル各種、各種シリンジ、テープ、その他
4	見守り用機器	バイタル機器（血圧、心拍数)、ホルスター心電計、ケーブルテレビ、テレビ電話、安否確認ボタン、その他

（2）管理項目

在宅医療、看護で使用する機器などは、衛生管理、保守も含めてサービス事業者等が管理する必要がある。

	項目	管理
1	医療機器の台帳管理	医療機器一台ごとに、所在情報、修理履歴の管理を行う。機器固有情報、システム構成品一覧、保守履歴一覧、機器写真や取扱説明書などの情報管理が必要。賃貸管理業務のため、バーコード発行を行い、機器に貼り付ける。購入／リース情報や減価償却情報、保守契約情報の

		登録も行うことで、資産台帳機能も持つ。
2	修理・点検・保守	保守スケジュール管理や保守履歴参照機能が必要である。各機器単位での作業経過の記録、修理使用部品、保守の原因・作業内容・保守結果、作業時間・作業費用故障写真等の履歴管理を行う。
3	貸出・返却管理	現場に貸し出している機器の管理機能であり、バーコードリーダ付き PDA など。
4	部品在庫管理	部品在庫の定数管理を行うことにより、発注点の把握とともに発注業務を行う。
5	使用状況管理	対象者宅で使用中の医療機器、医療衛生材料、見守り用機器につての使用状況の情報を管理しケアチームで共有する。

１１．運用管理規程について

以下は暫定記述である。見守り支援システム固有の規定項目の検討については、次年度の課題とする。

運用管理規程には、安全管理ガイドラインが要求する事項を満たす必要がある。特に、

・運用管理規程の作成・運用
・責任分界を定めた契約の締結
・ベンダが標準化に対する方針の確認
・ネットワークサービス事業者の選定における条件

など、を明確にし、文書化しておくことが重要である。

（1）運用規程の項目例

	項目	備考
1	第ｘ章　総則 （目的）（適用範囲）（ゲートウェイ等設備の設置）（対象情報）（規定の変更）	
2	第ｘ章　参加契約 （参加申込の方法）（参加申込の承諾）（参加申込の不承諾）（参契約に基づく権利の譲渡禁止等）（変更の届出）（途中解約）	
3	第ｘ章　管理体制 （情報管理責任機関）（センター設備に係る管理者の任命）（ゲートウェイ等設備に係る管理者の任命）（利用者の限定）（文書管理）（著作権の保護）（監査体制と監査責任者の任命）（問合せ対応）　（事故対応）（利用者への周知法）	
4	第ｘ章　管理者及び利用者の責務 （センター設備に係る管理者の責務）（ゲートウェイ等設備に係る管理者の責務）（監査責任者の責務）（利用者の責務）	
5	第ｘ章　一般管理における運用管理事項 （来訪者の記録・識別、入退の制限等の入退管理）（レジストリ、リポジトリ情報の記録媒体の管理（保管・授受等））（個人情報を含む媒体の廃棄の規程）（リスクに対する予防、発生時の対応）（利用制限）（サービス提供の中断）（システムへのアクセス制限、アクセス管理）	
6	第ｘ章　教育と訓練 （マニュアルの整備）（従業者に対する人的安全管理措置）	
7	第ｘ章　業務委託の安全管理措置 （業務委託契約における守秘条項）（システム改造及び保守でのデータ参照）	

8	第 x 章　ネットワーク接続に係る項目 （安全を技術的、運用的面から確認した文書の管理）（患者説明・患者同意）	

（２）運用規程の項目例

IHEのXDSを構築する際の合意事項のテンプレートの例を示す。

	項目	備考
1	A.1　はじめに	
2	A.2　用語	
3	A.3　参考資料	
4	A.4　組織的規約 （組織構成）（組織的規約）（資金提供）（透明性）（施行と是正）（法的問題；法的統治、義務とリスク配分、免責、発行物への知的財産権）	
5	A.5　運用規則 （サービスレベルの合意）（日常的運営）（システム停止の管理）（構成管理）（新機能要素の追加）（データ維持、保存、バックアップ）（不具合の回復）	
6	A.6　メンバーの規約 （入会）（メンバーのタイプ）（メンバーの方針）	
7	A.7　XAD の外部からの接続性 （相互運用性規約）	
8	A.8　システム構成 （業務アクタ）（技術アクタの仕様）	
9	A.9　用語と意味	
10	A.10 患者プライバシーと同意 （ドキュメントのアクセスと利用の一般則）（患者同意）（プライバシーを超える時のガイド）	
11	A.11　技術上のセキュリティ	

附属書 A　セキュリティガイドライン

はじめに

本附属書は、JIS Q 27001:2006（ISO/IEC 27001:2005）（ISMS 認証基準）および ISO/IS 27799（ISO/IEC 27001 を医療分野向けに特化したガイドライン）で定義される情報セキュリティ管理対策を示すものである。附属書 B を参考に当該システムに関する情報資産の洗い出しを行い、附属書 C が提示するリスクアセスメント手法を元に定義される実施すべき情報セキュリティ対策の例を提案している。

また本附属書では、医療・介護・福祉・健康に関する情報資産を「ヘルスケア情報」と定義し、見守りにおける包括的な情報セキュリティ対策のガイドラインとして利用されることを期待する。

【目次】

１．適用範囲 4

２．引用規格・引用文献 4

３．用語の定義 4

４．記号および略語 4

５．情報セキュリティ基本方針 4

５．１　情報セキュリティ基本方針の管理目的 4

５．１．１　情報セキュリティ基本方針文書 4

５．１．２　情報セキュリティ基本方針のレビュー 6

５．２　情報セキュリティのための組織 6

５．２．１　内部組織の管理目的 6

５．２．２　外部組織および第三者の管理目的 7

５．３ 資産の管理 8

５．３．１　資産に対する責任の管理目的 8

５．３．２　資産の分類の管理目的 8

５．４ 人的資源のセキュリティ 9

５．４．１　雇用前の管理目的 9

５．４．２　雇用期間中の管理目的 10

５．４．３　雇用の終了または変更の管理目的 10

５．５ 物理的及び環境的セキュリティ 11

５．５．１　セキュリティを保つべき領域の管理目的 11

５．５．２　装置のセキュリティの管理目的 11

５．６ 通信及び運用の管理 12

５．６．１　運用の手順及び責任の管理目的 12

５．６．２　第三者が提供するサービスの管理の管理目的 13

５．６．３　システムの計画作成及び受入れの管理目的 13

５．６．４　悪意あるコード及びモバイルコードからの保護の管理目的 14

５．６．５　バックアップの管理目的 14

５．６．６　ネットワークセキュリティ管理の管理目的 14

５．６．７　媒体の取扱いの管理目的 14

５．６．８　情報の交換の管理目的 15

５．６．９　電子商取引サービスの管理目的 16

５．６．１０　監視の管理目的 16

５．７ アクセス制御 17
５．７．１　アクセス制御に対する業務上の要求事項の管理目的 17
５．７．２　利用者アクセスの管理の管理目的 18
５．７．３　利用者の責任の管理目的 19
５．７．４　ネットワークのアクセス制御の管理目的 19
５．７．５　オペレーティングシステムのアクセス制御の管理目的 20
５．７．６　業務用ソフトウェア及び情報のアクセス制御の管理目的 21
５．７．７　モバイルコンピューティング及びテレワーキングの管理目的 21
５．８ 情報システムの取得、開発及び保守 21
５．８．１　情報システムのセキュリティ要求事項の管理目的 21
５．８．２　業務用ソフトウェアでの正確な処理の管理目的 22
５．８．３　暗号による管理策の管理目的 23
５．８．４　システムファイルのセキュリティの管理目的 23
５．８．５　開発及び支援プロセスにおけるセキュリティの管理目的 23
５．８．６　技術的ぜい弱性管理の管理目的 23
５．９ 情報セキュリティインシデントの管理 24
５．９．１　情報セキュリティの事象及び弱点の報告の管理目的 24
５．９．２　情報セキュリティインシデントの管理及びその改善の管理目的 24
５．１０ 業務継続管理 25
５．１０．１　事業継続管理における情報セキュリティの側面の管理目的 25
５．１１ コンプライアンス 25
５．１１．１　法的要求事項の順守の管理目的 25
５．１１．２　セキュリティ方針及び標準の順守、並びに技術的コンプライアンスの管理目的 26
５．１１．３　情報システム監査に対する考慮事項の管理目的 26

１．適用範囲

本附属書は、当該システムの情報セキュリティ管理の設計および実装に関して、詳細なセキュリティ対策を提示すものであり、情報システムのみならず情報資産を利用・管理する全ての人および施設を対象としている。

２．引用規格・引用文献

・JIS Q 27001:2006（ISO/IEC 27001:2005）: 情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項
・ISO/IS 27799：Health informatics -- Information security management in health using ISO/IEC 27002

３．用語の定義

・医療従事者
ある医療上の義務を果たすと認められた団体によって認可された資格を有する人。
・脅威
あるシステムや組織に対し望まれざる事件を引き起こす可能性となりうる原因のこと。
・情報セキュリティ
情報の機密性、完全性、可用性を維持すること、さらには真正性、説明可能性、否認できないこと、信頼性も含まれ得る。
・脆弱性
資産もしくは資産のグループが有する脅威に利用されうる弱点のこと。
・リスク
事象の可能性（もしくは、より頻繁に、ありそうなこと）と、その結果の組み合わせのこと。

４．記号および略語

特になし。

５．情報セキュリティ基本方針

５．１　情報セキュリティ基本方針の管理目的

５．１．１　情報セキュリティ基本方針文書

情報セキュリティ基本方針文書は、経営陣によって承認され、全従業員及び関連する外部関係者に公表し、通知することが望ましい。情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項、関連する法令及び規則に従って規定する。

個人情報を含むヘルスケア情報を取り扱う組織は、文書化されたセキュリティ基本方針が必要であり、それは経営陣によって承認され、公表され、全従業員と外部の関係団体に通知されなければならない。
地域医療連携や介護保健福祉においては、一般の情報セキュリティ基本方針の内容に加え、以下の要件を含ませることが望ましい。
a) ヘルスケア情報セキュリティの必要性
b) ヘルスケア情報セキュリティのゴール
c) 法令、規制、そして契約上の要求事項として、個人のヘルスケア情報の保護を含むもの、およびこれらの情報を保護するためのヘルスケア従事者の法的および倫理的な責任
d) 情報セキュリティ事件の通知のアレンジとして、非難や報復の恐れなしに機密性への懸念を提出するチャンネルを含むもの

さらに、医療分野や介護保健福祉、地域医療連携それぞれの特性において、以下の要因についての考慮が必要である。
a) ヘルスケア情報の広がり
b) 従業員の権限と倫理的な責任、法律と専門化団体で合意されたもの
c) 患者の権利、プライバシーと彼らの記録へのアクセスに適用できるもの
d) 患者の同意を得ることと患者の機密を維持することに関する臨床医の義務
e) 患者の診療が第一義であるときに、通常のセキュリティに関する取り決めを打ち負かすことのできる臨床医と医療機関の適法の必要性、しばしば患者が彼らの意向を表現できないことと同盟を結ぶ、これを達成するために採用されるべき手順と同様にそれを必要とする
f) 医療が「分担医療」もしくは「拡張医療」を基礎として提供されるところにおける、それぞれの医療機関、および患者の義務
g) 研究と医療裁判を目的とした情報共有に適用される取り決めと手順
h) 臨時代替医師や学生、オンコール・スタッフのような一次的な従業員の配置と認可権限
i) 聖職者や慈善事業者のような、ボランティアやサポートスタッフによる個人ヘルスケア情報へのアクセスの配置とその制限

なお、個人データが国家もしくは司法権の境界を越えるケースでは、ISO 22857 ("Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health information") が適用されることが望ましい。

５．１．２　情報セキュリティ基本方針のレビュー

情報セキュリティ基本方針は、１年ごとなどあらかじめ定める間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当、及び有効であることを確実にするためにレビューすることが望ましい。

レビューの際には、以下の要素を含ませることが望ましい。

a)　医療機関の運用変更の性質と、それによるリスク・プロファイルとリスク管理の要求事項

b)　組織の IT インフラへの変更、これらの変更が組織のリスク・プロファイルにもたらした変更

c)　組織のリスク･プロファイルに同様に影響を与える外部環境において識別された変更

d)　最新の管理策、適合性、国家の医療団体の要望／協定への保証、そして国際的もしくは大陸的な特性を含む新しい法令／法的義務

e)　ヘルスケア専門者の協会と個人ヘルスケア情報の保護に関する情報責任者からの最新のガイダンスと推奨事項

f)　法廷で審議された判例、それゆえに先例を築いたり破棄したり、実例を築いたりしたもの

g)　スタッフ、患者およびそのパートナー、その診療者、研究者、そして政府（たとえば、プライバシー責任者）などによって、組織に表現された基本方針に関する事項

５．２　情報セキュリティのための組織

５．２．１　内部組織の管理目的

５．２．１．１　情報セキュリティに対する経営陣の責任

個人ヘルスケア情報の管理者である組織において、管理の説明責任は本質的である。責任と調停は、組織が明確な情報セキュリティのインフラを持つことによってのみ、長期間に亘って維持されうる。経営陣は、情報セキュリティの責任に関する明りょうな方向付け、自らの関与の明示、責任の明確な割当て及び承認を通して、組織内におけるセキュリティを積極的に支持すること。

５．２．１．２　情報セキュリティの調整

情報セキュリティに関する活動では、情報セキュリティの責任を明確に定義し、アサインすること。

５．２．１．３　情報セキュリティ責任の割当て

すべての情報セキュリティ責任を、明確に定めること。

５．２．１．４　情報処理設備の認可プロセス

新しい情報処理設備に対する経営陣による認可プロセスを定め、実施すること。

５．２．１．５　秘密保持契約

情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューすること。

５．２．１．６　関係当局との連絡

関係当局との適切な連絡体制を維持すること。医療機関は、相互運用を可能とするために、それらの共同で合意された管理策を実装しなければならない。

５．２．１．７　専門組織との連絡

情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持すること。

５．２．１．８　情報セキュリティの独立したレビュー

情報セキュリティ及びその実施のマネジメントに対する組織の取組み（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）は、あらかじめ定められた間隔で、又はセキュリティの実施に重大な変化が生じた場合に、独立したレビューを実施すること。

５．２．２　外部組織および第三者の管理目的

５．２．２．１　外部組織に関係したリスクの識別

外部組織がかかわる業務プロセスからの、組織の情報及び情報処理施設に対するリスクを識別し、外部組織にアクセスを許可する前に適切な管理策を実施すること。ヘルスケア情報を取り扱う組織は、外部組織（たとえば、契約を受けた保守会社）によって、これらのシステムやそこに含まれるデータにアクセスされることに起因するリスクを評価しなければならない。また、リスクの識別されたレベルと採用されたテクノロジに相応しいセキュリティ管理策を実装しなければならない。

５．２．２．２　顧客対応におけるセキュリティ

利用顧客が組織の情報又は資産にアクセスする前に、明確にしたすべてのセキュリティ要求事項に対処すること。

５．２．２．３　第三者との契約におけるセキュリティ

組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理に関わる第三者との契約、又は情報処理施設に製品・サービスを追加する第三者との契約は、関連するすべてのセキュリティ要求事項を取り上げること。第三者によるサービス、そこでは個人ヘルスケア情報を取り扱う機関は、下記に言及する正式な契約書を採用しなければならない。

a)　機密性の特性、および個人ヘルスケア情報の価値
b)　実装され、集められるべきセキュリティ手段
c)　第三者によるこれらのサービスへのアクセスの制限
d)　提供されるサービス全体として達成されるべきサービスレベル

e)　医療機関の ISMS への報告の形式と頻度
f)　適切な医療機関会合と作業部会における第三者の表現の取り決め
g)　第三者の適合性監査のための取り決め
h)　罰則に関する取り決め
　これらの要求事項は、個人ヘルスケア情報の、機密性、完全性、可用性が維持されることを確かめること意図する。

５．３ 資産の管理
５．３．１　資産に対する責任の管理目的
　地域医療連携や介護保健福祉において個人ヘルスケア情報を取り扱う場合は、一般の情報セキュリティ基本方針の内容に加え、以下の要件を含ませることが望ましい。
a)　ヘルスケア情報資産の説明（資産の台帳の維持）
b)　それぞれのヘルスケア情報資産に対して、責任があると識別され管理が任命されたメンバーを設定すること
c)　当該の情報資産は識別され、文書化され、実装された、受諾可能な利用に関するルールを持つこと
　ヘルスケア情報を取り扱う組織は、これらの資産の流通、およびこれらの資産の完全性を維持するためのルールを持つことが望ましい。

５．３．１．１　資産目録
　すべての資産を明確に識別し、また、重要な資産すべての目録を作成し維持すること。
５．３．１．２　資産の保有者
　情報及び情報処理施設と関連する資産のすべてについて、組織のなかに、その保有者を指定すること。
５．３．１．３　資産利用の許容範囲
　情報及び情報処理施設に関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施すること。

５．３．２　資産の分類の管理目的
５．３．２．１　分類の指針
　情報は、組織に対しての価値、法的要求事項、取り扱いに慎重を要する度合い及び重要性の観点から分類すること。ヘルスケアにおける情報資産のための保護レベルを決定することは複雑であり、政府のデータ分類との比較は誤解を招きうる。次に挙げるのは、ヘルスケアにおける情報の重要な特質である。
a)　個人ヘルスケア情報の機密性は主観的である。すなわち、はデータの主体（要す

るに利用者）のみが、データのいろいろなフィールドやグループの相対的な機密性について、適切な決定を下す権限を有することを可能にしなければならないことがある。

b)　個人ヘルスケア情報の機密性は、状況に依存する。たとえば、病院の救急部門がアクセスを許された利用者の名前と住所のリストは、その利用者には特に機密であるとは考えられないかもしれないが、同じ名前と住所が重度の症状を取り扱うクリニックのリストにあれば、その利用者にとって機密度が高いと考えられるかもしれない。

c)　個人ヘルスケア情報の機密性は、記録の障害やその対策にために移すことができる。個人ヘルスケアデータと情報を取り扱う組織は、そのようなデータを一律に機密であると選択してもよいかもしれない。

情報資産が機密であると識別し、適切なラベリングを付することは、必要なセキュリティ対策の標識として、また従業員の訓練と基本方針への適合性において、重要である。それもまた、管轄権、第三者組織およびそのスタッフの間での、データ保護合意の重要な構成要素であるかもしれない。

可用性と完全性の程度がヘルスケアの提供にとって本質的な方針となる。そのような厳密さの分類もまた、プロセス、IT デバイス、ソフトウェア、人の配置に適用され得る。厳密さはリスク評価を通して識別されなければならない。

５．３．２．２　情報のラベル付け及び取扱い

情報に対するラベル付け及び取扱いに関する適切な一連の手順は、組織が採用した分類体系に従って策定し、実施すること。すべての個人ヘルスケア情報を取り扱う情報システムは、利用者に個人ヘルスケア情報の機密性について、システムのスタートアップまたはログオン時点から通知することが望ましい。そして、個人ヘルスケア情報を含むハードコピーを出力する際にはラベル付けをすることが望ましい。

５．４ 人的資源のセキュリティ

５．４．１　雇用前の管理目的

５．４．１．１　役割及び責任

個人ヘルスケア情報を取り扱うスタッフがいるすべての組織は、そのような関連のある業務を文書化することが望ましい。セキュリティ上の役割と責任もまた、組織の情報セキュリティ基本方針に含まれるのと同様に、関連する業務の記述の中に文書化されることが望ましい。

臨時代替医師や学生、医学研修生のような、一時的、または短期のスタッフに対する役割と責任には、特別の配慮が払われる必要がある。

５．４．１．２　選考

スタッフ、契約者、もしくはボランティアが個人ヘルスケア情報を取り扱うすべての組織は、最低でも、業務を適用する際には、身元と住所と以前の雇用を確かめることが望ましい。

５．４．２　雇用期間中の管理目的

従業員、契約相手及び第三者の利用者の、情報セキュリティの脅威及び諸問題、並びに責任及び義務に対する認識を確実なものとし、通常の業務の中で組織の情報セキュリティ基本方針を維持し、人による誤りのリスクを低減できるようにすること。

個人ヘルスケア情報を取り扱うすべての組織は、個人ヘルスケア情報を取り扱う従業員の雇用期間と条件を、従業員の情報セキュリティ基準に対する契約に含むことが望ましい。

雇用の期間と条件は下記のようになっていることが望ましい。

a)　情報セキュリティ基本方針に対する違反が識別された場合の罰則

b)　利用者の機密に関連する条件が雇用の完了まで永久に存続することを確かめること

ヘルスケアスタッフに関しては、雇用の期間と条件は、そのようなスタッフが利用者の記録と関連するヘルスケア情報システムの何のアクセス権を持つかを、第三者からの請求があったときに示すことができる体制作りが必要となる。

５．４．２．１　経営陣の責任

経営陣は、情報セキュリティインシデントや、従業員の雇用に関して責任を持たなければならない。

５．４．２．２　情報セキュリティの意識向上、教育及び訓練

従業員に対して情報セキュリティの教育と訓練を行わなければならない。そして手続は個人ヘルスケア情報を取り扱う全ての従業員のみならず、関連のある第三者の契約者、研究者、学生、そしてボランティアに提供されていること。

５．４．２．３　懲戒手続

情報セキュリティの違反に対しては、医療機関の訓練のプロセスは基本方針に従うべきである。さらには適用可能な法律と、ヘルスケア従事者とヘルスケア従事者団体の間の合意に従わなければならない。

５．４．３　雇用の終了または変更の管理目的

５．４．３．１　雇用の終了又は変更に関する責任

雇用の終了又は変更に関する責任は、明確に定義し、割り当てること。

５．４．３．２　資産の返却

ヘルスケアにおいては、多くのスタッフのクラス、たとえば医師と看護師などの交代は頻発し得る。交代後の業務に不必要な資産は、速やかに管理主体に返却されなければならない。

５．４．３．３　アクセス権の削除

個人ヘルスケア情報を取り扱うすべての組織は、それらの情報を取り扱う、恒久的、もしくは一時的な従業員、第三者契約者、またはボランティアのアクセス権を、その雇用もしくはボランティア活動の終了とともに、可能な限り速やかに終了させなければならない。必要でないアカウントや権限は、組織の雇用を離れるのと同じ方法で終了されることが望ましい。

医療機関は、辞職の通知、解雇等に引き続いて、アクセス権の即座の終了を深刻に考慮することが求められる。

５．５ 物理的及び環境的セキュリティ

５．５．１　セキュリティを保つべき領域の管理目的

５．５．１．１　物理的セキュリティ境界

個人ヘルスケア情報を取り扱う組織は、情報処理施設を含む領域を保護するために、セキュリティ境界を設定することが望ましい。これらのセキュリティ領域は、認可された人員だけがアクセスを許されるよう適切な入室制御によって、保護されることが望ましい。

５．５．１．２　物理的入退管理策

個人のヘルスケア情報を処理する組織は、物理的な制約と施設への入退ルールを設定することが望ましい。

５．５．１．３　オフィス、部屋及び施設のセキュリティ

５．５．１．２に順ずる。

５．５．１．４　外部及び環境の脅威からの保護

５．５．１．２に順ずる。

５．５．１．５　セキュリティを保つべき領域での作業

５．５．１．２に順ずる。

５．５．１．６　一般の人の立寄り場所及び受渡し場所

ヘルスケアの提供は、大量の機微な情報へのアクセスを可能とする。それらのヘルスケアにおける物理的な領域、すなわち、ヘルスケア情報をインタビューやデータを見ることのできるシステムによって収集しているところでは、さらなるセキュリティ対策が求められる。

利用者のプライバシーの責務を全うするためには、ヘルスケアではそのような通知と注意が、エレベータやインタビューがなされている部屋のドアや、その他の領域に掲示されることが望まれる。

５．５．２　装置のセキュリティの管理目的

５．５．２．１　装置の設置及び保護

地域医療連携や介護保健福祉において個人ヘルスケア情報を取り扱う場合は、一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報にアクセスできるワークステーション等を、患者や公衆による意図しない閲覧を防ぐように設置することが望ましい。

５．５．２．２　支援ユーティリティ

ネットワーク配線とその操作は、逆に接触する材質と放射による影響を受けうる。例えば放射線を取り扱う医療機関では、リスクが高く高放射の領域におけるネットワークとその他の配線に厳重な配慮を払うことが望ましい。

５．５．２．３　ケーブル配線のセキュリティ

５．５．２．１に順ずる。

５．５．２．４　装置の保守

５．５．２．１に順ずる。

５．５．２．５　構外にある装置のセキュリティ

一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報を取り扱う組織は、データを記録したりレポートしたりする医療機器の、その敷地外におけるいかなる利用について、正式かつ特別に権限を与えることが望ましい。これには遠隔地の操作者から利用される設備を含めることが望ましい。

５．５．２．６　装置の安全な処分又は再利用

ヘルスケア情報用の業務用ソフトウェアを取り扱う組織は、ヘルスケア情報、業務用ソフトウェア、または個人ヘルスケア情報を含む全ての媒体を利用する必要性がなくなったとき、セキュアに上書きまたは破壊することが望ましい。操作を簡単にするために、医療機関は全ての媒体を上書きすることなどの対策が望ましい。

５．５．２．７　装置の移動

装置、データ、もしくは個人ヘルスケア情報を含むヘルスケア用の業務用ソフトウェアをサポートするソフトウェアを提供したり、利用したりする組織は、そのような装置、データもしくはソフトウェアが、組織の認可なしに廃棄されたり設置されたりすることを許可しないことが望ましい。

５．６ 通信及び運用の管理

５．６．１　運用の手順及び責任の管理目的

５．６．１．１　操作手順書

操作手順は、文書化して維持していくこと。また、その手順は、必要とするすべての利用者および従業員に対して利用可能とすること。

５．６．１．２　変更管理

個人ヘルスケア情報に対して変更を行うためには慎重を有する。それゆえ、一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報を取り扱う組織は、正

式かつ構造的な変更制御手順によって、変更を制御することが望ましい。この変更手続きは明白に記録され、変更に関わるリスクを評価してあることが望ましい。

５．６．１．３　職務の分離

個人ヘルスケア情報を取り扱う組織は、実現可能な範囲で職務と責任の領域分離することが望ましい。これは個人ヘルスケア情報への権限のない変更、または誤った利用の機会を減らすためである。

５．６．１．４　開発施設、試験施設及び運用施設の分離

個人ヘルスケア情報を取り扱う組織は、仮想的もしくは物理的に開発、試験、そして運用施設を分離しなければならない。ソフトウェアの開発中から運用へのステータスの移行のためのルールは、これらを取り扱う組織によって、定義され文書化されなければならない。

５．６．２　第三者が提供するサービスの管理の管理目的

５．６．２．１　第三者が提供するサービス

第三者が提供するサービスに関する合意に含まれるセキュリティ管理策、サービスの定義、及び提供サービスレベルが、第三者によって実施、運用及び維持されることを確実にすること。

５．６．２．２　第三者が提供するサービスの監視及びレビュー

第三者が提供するサービス、報告及び記録は、常に監視し、レビューすること。また、監査も定期的に実施すること。

５．６．２．３　第三者が提供するサービスの変更に対する管理

関連する業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、サービス提供の変更（現行の情報セキュリティ方針、手順、及び管理策の保守・改善を含む）を管理すること。

５．６．３　システムの計画作成及び受入れの管理目的

５．６．３．１　容量・能力の管理

要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測すること。

５．６．３．２　システムの受入れ

一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報を取り扱う組織は、計画された新しい情報システム、更新、そして新しいバージョンのための受け入れ基準を確立し、そして受け入れに先立って適切な試験を実行しなければならない。それらの試験の範囲と厳格さは、その変更に関わる識別されたリスクに対応したレベルに設定されなければならない。

５．６．４　悪意あるコード及びモバイルコードからの保護の管理目的

５．６．４．１　悪意のあるコードに対する管理策

一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報を取り扱う組織は、悪意あるソフトウェアから保護するために、マルウェア等の適切な検出と防止の制御機能を実装しなければならない。そしてユーザへの適切な通知手段を実装しなければならない。

デバイスが悪意あるコードに感染したことが検知、もしくはその疑いがある場合には、それはネットワークから切り離されなければならない。また、それに接続されているあらゆるヘルスケアデバイスも同様に切り離され、評価のための優先度がルール化されなければならない。

５．６．４．２　モバイルコードに対する管理策

モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティルールに従って動作することを確実にする環境設定を行うこと。また、認可されていないモバイルコードを実行できないようにすること。

５．６．５　バックアップの管理目的

５．６．５．１　情報のバックアップ

個人ヘルスケア情報を取り扱う組織は、全ての個人ヘルスケア情報をバックアップし、その将来の利用に備えて物理的にセキュアな環境に保管しなければならない。

５．６．６　ネットワークセキュリティ管理の管理目的

５．６．６．１　ネットワーク管理策

ネットワークを脅威から保護するために、また、処理中の情報を含め、ネットワークを用いた業務用システム及び業務用ソフトウェアのセキュリティを維持するために、ネットワークを適切に管理し、制御すること。

５．６．６．２　ネットワークサービスのセキュリティ

個人ヘルスケア情報を取り扱う組織は、全面的なネットワークサービスの機能不全もしくは性能の低下がサービスの実施に与えるインパクトを注意深く考慮することが望ましい。そして適切な設備と事業継続計画を提供しなければならない。

５．６．７　媒体の取扱いの管理目的

５．６．７．１　取り外し可能な媒体の管理

一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報を取り扱う組織は、媒体に保存されている個人ヘルスケア情報に関して、以下の事項を確認することが望ましい。

a)　媒体の搬送中には暗号化されていること

b)　媒体の搬送中には盗難対策がなされていること

暗号化されていない個人ヘルスケア情報を含む媒体の物理的な状態と所在は監視されなければならない。そして媒体のログは維持されることが望ましい。

５．６．７．２　媒体の処分

全ての個人ヘルスケア情報は、それを格納する媒体が破壊される前にセキュアにゼロ情報や乱数などで上書きされなければならない。これは関連する装置を修理や処分にきわめて重要である。

５．６．７．３　情報の取扱手順

情報の取扱い及び保管についての手順は、その情報を認可されていない開示又は誤用から保護するためにルール化すること。

５．６．７．４　システム文書のセキュリティ

システム文書は、認可されていないアクセスから保護すること。

５．６．８　情報の交換の管理目的

５．６．８．１　情報交換の方針及び手順

ヘルスケア情報の交換方針に特化したガイダンスは「ISO 22857：医療情報 – 個人医療情報の境界を越えてのやり取りを用意にするためデータ保護に関するガイドライン」に見出すことができる。この標準は個人医療情報の境界を越えてのやり取りについて明確に言及しているが、その多くの助言は１つの施設から他の施設へのデータの交換を取り扱う必要があるところに適合されうるものである。

５．６．８．２　情報交換に関する合意

他の機関とのヘルスケア情報の交換を許容する機関は、そのような交換を独自のセキュリティ方針をもって制御しなければならない。そして評価されたリスクを元にして制御の枠組みを確立しなければならない。組織は「接続の規約」もしくは同等のものを考慮することが望ましい。

組織はこれらの情報の交換におけるセキュリティが、適合性監査の主題であることを明らかにしなければならない。

５．６．８．３　配送中の物理的媒体

情報を格納した媒体は、組織の物理的境界を越えた配送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。

５．６．８．４　電子的メッセージ通信

個人ヘルスケア情報を電子メールでやり取りしている組織は、配送中におけるその機密性、そして届いたときの完全性を確認するために段階を踏むことが望ましい。
個人ヘルスケア情報を含む電子メールは、配送の際に PKI などの技術を利用して暗号化されることが望ましい。

利用者に関する個人ヘルスケア情報が電子メールで送られたり、ファックスされた

り、電話での会話において伝えられたり、その医療機関の外部の団体と交換されたりする前に、患者の同意がとられることが望ましい。

５．６．８．５　相互接続される業務用情報システム

業務用情報システムの相互接続と関連がある情報を保護するために、個別方針及び手順を策定し、実施すること。

５．６．９　電子商取引サービスの管理目的

５．６．９．１　電子商取引

公衆ネットワークを経由する電子商取引に含まれる情報は、不正行為、契約紛争、認可されていない開示及び改ざんから保護すること。

５．６．９．２　オンライン取引

オンライン取引に含まれる情報は、不完全な通信、誤った通信経路設定、認可されていないメッセージの変更、認可されていない開示、認可されていない複製又は再生を未然に防止するために、保護すること。

５．６．９．３　公共的に利用可能なヘルスケア情報

公共的に利用可能なヘルスケア情報はアーカイブされ、完全性が保護されることが望ましい。また、当該ヘルスケア情報のソースが明言され、損耗から保護されることが望ましい。

５．６．１０　監視の管理目的

個人ヘルスケア情報を保護する上での全てのセキュリティ要求事項において最も重要なものは、監査とロギングである。これらは自らの情報を電子システムに委託する患者のための説明可能性を明らかにし、そのようなシステムの利用者に、これらのシステムの受容可能な利用の方針を確認することの強い動機を提供する。効果的な監査とロギングは、ヘルスケア情報システムもしくは個人ヘルスケア情報の誤った利用を抽出することを目的とし、組織と患者が特権を悪用する不正を検知する手助けとなりうる。

５．６．１０．１　監査ログ取得

個人ヘルスケア情報を取り扱うヘルスケア情報システムは、利用者によるアクセス、更新、もしくはシステムを経由した個人ヘルスケア情報のアーカイブの度にセキュアな監査記録を作成することが望ましい。監査ログは、その利用者をユニークに識別し、データ主体（すなわち、利用者）をユニークに識別し、利用者によって実行された機能（記録作成、アクセス、更新、その等）と、それが実施された日時を識別できることが望ましい。

利用者のデータが更新されるとき、以前のデータ内容の記録と、関連する監査レコード（誰がいつそのデータを入力したか）が記録されることが望ましい。

個人ヘルスケア情報を含むメッセージを配送するために使われるメッセージング・システムは、メッセージ配送のログを保持することが望ましい。組織は、これら監査ログの保持期間を決定することが望ましい。

５．６．１０．２　システム使用状況の監視

ヘルスケア情報システムの監査ロギング機能は、ヘルスケア情報システムが監査されている間はいつでも機能していなければならない。

個人ヘルスケア情報を含むヘルスケア情報システムは、ログと監査証跡の解析機能を提供することが望ましい。

a)　指定された利用者レコードの指定された期間について、アクセスもしくは更新した全てのシステム利用者の識別を行う。

b)　指定されたシステム利用者について、指定された期間に、記録にアクセスされた、もしくは更新された全ての利用者を識別する。

システムもしくは監査ロギングシステムがそのような機能を提供するところでは、組織はあらゆる予測および警告の機能を利用することが望ましい。

５．６．１０．３　ログ情報の保護

監査記録へのアクセスはセキュアかつ改ざん検知できる形で行われなければならない。そしてシステム監査ツールと監査証跡へのアクセスは、誤使用またはその疑いを招くことを防ぐよう対策されていなければならない。

５．６．１０．４　実務管理者及び運用担当者の作業ログ

システムの実務管理者及び運用担当者の作業は、記録すること。

５．６．１０．５　障害のログ取得

障害のログを取得し、分析し、また、障害に対する適切な処置を講じること。

５．６．１０．６　クロックの同期

組織又はセキュリティ領域内の関連するすべての情報処理システム内のクロックは、合意された正確な時刻源と同期させること。

５．７ アクセス制御

５．７．１　アクセス制御に対する業務上の要求事項の管理目的

個人ヘルスケア情報を取り扱う組織は、そのような情報へのアクセスを制御しなければならない。一般に、ヘルスケア情報システムの利用者は個人ヘルスケア情報にのみアクセスすることが望ましい。

a)　利用者とデータ主体の間に医療提供関係が存在するとき

b)　利用者がデータ主体のために何らかの行為を行っているとき

c)　ここ行為をサポートするために、特定のデータの需要があるとき

５．７．１．１　アクセス制御方針

個人ヘルスケア情報を取り扱う組織は、データへのアクセスを統治するアクセス制

御方針を持たなければならない。アクセス制御に関する組織の方針は、予め定義されたロールをベースとして確立されることが望ましい。そのロールはロールの必要に合致した、しかし制限された権限に関連付けられているものとする。

医療の場合においては、明確な方針と手順のための通常よりも強い要望がある。医療の提供が遅延したり妨げられたりしないように、緊急の状況において「通常」のルールを上書きすることのようなものである。

５．７．２　利用者アクセスの管理の管理目的

５．７．２．１　利用者登録

ヘルスケア情報システムの利用者登録作業に下記を含めることが望ましい。

a) 利用者識別の正確な入手
b) 確認後における利用者が有する専門的資格の正確な入手、および/または、職名
c) 個人の顔のデジタル画像、もしくは他の生態計測情報
d) 明瞭な利用者識別の割り当て

ヘルスケア情報システムへのアクセスは、正式な利用者登録の手続きを経なければならない。利用者登録の手続きは、提供された利用者識別のレベルが、その利用者が利用可能になるアクセスのレベルに合致していることを確認しなければならない。
利用者登録の詳細は、それらが完全で、正確で、そのアクセスが必要であることが、定期的にレビューされなければならない。

５．７．２．２　特権管理

アクセス制御を実装および運用することは、個人ヘルスケア情報における機密性、可用性、そして完全性を確認することに対して重要である。それらは下記のとおりである。

a) ロールを基礎としたアクセス制御。
b) ワークグループ基礎としたアクセス制御。
c) 自由裁量のアクセス制御。

ヘルスケア情報システムは、ロールを基礎としたアクセス制御（RBAC と呼ばれることがある）をサポートすることが望ましい。それは、各利用者を１つもしくはそれ以上のロールに対応付けることができ、それぞれのロールは１つもしくはそれ以上のシステム機能に対応付けられる。

個人ヘルスケア情報を含むヘルスケア情報システムの１人の利用者は、そのサービスに単一のロール（すなわち、１つ以上のロールで登録された利用者は各ヘルスケア情報システムへのアクセスセッションにおいて単一のロールを選択することが望ましい）でアクセスしなければならない。利用者のロールの異なる様相を反映するために、適切で、特別なロールが作成されることが望ましい。これらは必要がなくなれば、即座に削除されることが望ましい。

ヘルスケア情報システムは従業員（ヘルスケア従事者、サポートスタッフ、その他含む）を利用者の記録に関連付け、そしてこの関連を元にした将来のアクセスを許可することが望ましい。

５．７．２．３　利用者パスワードの管理

ヘルスケアの提供現場に見られる時間的な制約として、パスワードをタイプすることが困難であること、また複数のパスワードを効果的に採用することが困難であることが知られている。それゆえ組織は PKI ベースのカード、生体認証、その他の技術を、この問題を解決するために考慮することが望ましい。

５．７．２．４　利用者アクセス権のレビュー

一般の情報セキュリティ基本方針の内容に加え、救急医療を提供し、緊急の状況で個人ヘルスケア情報へのアクセスが必要になる場合は、特別な配慮が必要である。そのような場合には、利用者は同意することができないかもしれないし、効果的なヘルスケアの提供を受けるために必要なシステムへのアクセス権を持っていないかもしれないことを考慮すること。

５．７．３　利用者の責任の管理目的

一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報を取り扱う組織は、利用者の責任を決定する際に、法的準拠性など、権利とヘルスケア従事者としての倫理的な責任を尊重することが望ましい。

５．７．３．１　パスワードの利用

パスワードの選択及び利用に際して、正しいセキュリティ慣行に従うことを、利用者に要求すること。

５．７．３．２　無人状態にある利用者装置

組織は、無人状態にある装置が適切な保護対策を備えていることを確実にすること。

５．７．３．３　クリアデスク・クリアスクリーン方針

書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用すること。

５．７．４　ネットワークのアクセス制御の管理目的

５．７．４．１　ネットワークサービスの利用についての方針

利用することを許可したサービスへのアクセスだけを、利用者に提供すること。

５．７．４．２　外部から接続する利用者の認証

遠隔利用者のアクセスを管理するために、適切な認証方法を利用すること。

５．７．４．３　ネットワークにおける装置の識別

特定の場所及び装置からの接続を認証するための手段として、自動の装置識別を考慮すること。

５．７．４．４　遠隔診断用及び環境設定用ポートの保護

診断用及び環境設定用ポートへの物理的及び論理的なアクセスは、制御すること。

５．７．４．５　ネットワークの領域分割

情報サービス、利用者及び情報システムは、ネットワーク上、グループごとに分割することが望ましい。

５．７．４．６　ネットワークの接続制御

共有ネットワーク、特に、組織の境界を越えて広がっているネットワークについて、アクセス制御方針及び業務用ソフトウェアの要求事項に沿って、利用者のネットワーク接続能力を制限すること。

５．７．４．７　ネットワークルーティング制御

コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、ルーティング制御の管理策をネットワークに対して実施すること。

５．７．５　オペレーティングシステムのアクセス制御の管理目的

５．７．５．１　セキュリティに配慮したログオン手順

オペレーティングシステムへのアクセスは、セキュリティに配慮したログオン手順によって制御すること。

５．７．５．２　利用者の識別及び認証

すべての利用者は、各個人の利用ごとに一意な識別子（利用者 ID）を保有すること。また、利用者が主張する同一性を検証するために、適切な認証技術を選択すること。

５．７．５．３　パスワード管理システム

パスワードを管理するシステムは、対話式とすること、また、良質なパスワードを確実とするものであること。

５．７．５．４　システムユーティリティの使用

システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理すること。

５．７．５．５　セッションのタイムアウト

一定の使用中断時間の経過したときは、使用が中断しているセッションを遮断すること。

５．７．５．６　接続時間の制限

リスクの高い業務用ソフトウェアに対しては、更なるセキュリティを提供するために、接続時間の制限を利用すること。

５．７．６　業務用ソフトウェア及び情報のアクセス制御の管理目的

５．７．６．１　情報へのアクセス制限

ヘルスケア情報システムは、利用者を認証しなければならず、それを少なくとも２つの要素を含む認証方法によって行うことが望ましい。情報へのアクセスは、個人のロールに基づいて承認されることが望ましい。

ヘルスケア情報システムにおいては、それらの利用者はセキュアに認証されるような技術的な方策、そのような方策が特にハンディキャップのある利用者に簡単に利用できること、そしてその他の第三者（たとえば介護人）によるアクセスを提供すること、に対する特別な考慮がなされることが望ましい。

５．６．６．２　取扱いに慎重を要するシステムの隔離

取扱いに慎重を要するシステムは、専用の隔離されたコンピュータ環境を持つこと。

５．７．７　モバイルコンピューティング及びテレワーキングの管理目的

５．７．７．１　モバイルコンピューティング及び通信

一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報を取り扱う組織は、以下を行うことが望ましい。

a)　ヘルスケアにおける移動型計算処理に関する特別な評価

b)　無線デバイスを含む移動型計算処理デバイスを利用する際において、とるべき警戒についての方針を用意すること

c)　それらの移動型の利用者に対して、方針への遵守を要望すること

d)　方針に対する利用者の遵守を監査すること

移動型機器による無線通信には、無線通信と同様ではあるが、情報セキュリティのためのいくつか追加の要望事項がある。WEP（Wired Equivalent Privacy）のように、いくつかの無線暗号化プロトコルには、それらを広範囲に無効化する生来の弱点を持つものがある。さらにその上、移動型デバイスに蓄積された情報は、いつもバックアップされるとは限らない。これは、ネットワークの帯域が制限されていたり、デバイスがバックアップの予定されている時間に接続されていなかったりするためである。

５．７．７．２　遠隔作業（テレワーキング）

個人ヘルスケア情報を取り扱う組織は、以下を行うことが望ましい。

a)　遠隔作業の際の行われる警告に関する方針を用意し実施する

b)　それらの付随する遠隔作業者を確認する

５．８ 情報システムの取得、開発及び保守

５．８．１　情報システムのセキュリティ要求事項の管理目的

５．８．１．１　セキュリティ要求事項の分析及び仕様化

新しい情報システム又は既存のシステムの改善に関する業務上の要求事項を記述し

た文書では、セキュリティの管理策についての要求事項を仕様化すること。

５．８．２　業務用ソフトウェアでの正確な処理の管理目的

個人ヘルスケア情報を取り扱うヘルスケア情報システムは、下記を行わなければならない。

a)　個々のサービスまたは治療の主体がシステム内でユニークに識別されることを確実にすることが設計されること

b)　意図せずに、または緊急の状況において、同じサービスまたは治療の主体のための重複もしくは複数の記録を併合できること

緊急治療の提供および、これまで十分な患者の識別が可能ではなかったかもしれない状況は、必然的に同一患者の複数の記録を作成する。いくつかの実施例では、全てのシステムにおいて、複数の患者記録をひとつの記録に併合することを許可される。そのような併合は、注意を必要とし、個人的な訓練だけではなく、技術的なツールをも必要とする。それにより元の記録から全体への情報の統合が容易になる。

個人ヘルスケア情報を取り扱う組織は、完全に可能とするために、個人情報の露見の機会を最小にする必要がある。

５．８．２．１　入力データの妥当性確認

業務用ソフトウェアに入力するデータは、正確で適切であることを確実にするために、その妥当性を確認すること。

５．８．２．２　内部処理の管理

処理の誤り又は故意の行為によって発生する情報の破壊を検出するために妥当性確認の機能を業務用ソフトウェアに組み込むこと。

５．８．２．３　メッセージの完全性

業務用ソフトウェアの真正性を確実にするための要求事項及びメッセージの完全性を保護するための要求事項を特定し、また、適切な管理策を特定し実装すること。

５．８．２．４　出力データの妥当性確認

個人ヘルスケア情報を取り扱うヘルスケア情報システムは、抽出されたデータが確実にその利用者の情報であることを保証しなければならない。

利用者を存在する記録に合致させることは、システム的に困難であるが、システムへ利用時の認証を強化することで実現できる。

ヘルスケア従事者がシステムを、それぞれの取り出された記録が利用者と一致し、必要な情報を提供すると信用することができることを確かなものとするために、システムの設計には大きな注意が払われる必要がある。

ヘルスケア情報システムは、プリントアウトのハードコピーが完了していることをチェックすることが可能であるようにすることが望ましい。

５．８．３　暗号による管理策の管理目的

５．８．３．１　暗号による管理策の利用方針

ヘルスケアにおけるデジタル証明書の発行および利用の方針、および鍵の管理に関する追加のガイダンスは、PKI に関する ISO 技術仕様３分冊のうちのパート３、すなわち ISO/TS/17090-3:医療情報―公開鍵基盤―認証局の方針管理、を参照すること。

５．８．３．２　かぎ（鍵）管理

５．８．３．１に順ずる。

５．８．４　システムファイルのセキュリティの管理目的

５．８．４．１　運用ソフトウェアの管理

運用システムに関わるソフトウェアの導入を管理する手順を備えること。

５．８．４．２　システム試験データの保護

個人ヘルスケア情報を取り扱う組織は、実際の個人ヘルスケア情報をテストデータとして利用しないことが望ましい。

５．８．４．３　プログラムソースコードへのアクセス制御

プログラムソースコードへのアクセスは、制限すること。

５．８．５　開発及び支援プロセスにおけるセキュリティの管理目的

５．８．５．１　変更管理手順

変更の実施は、正式な変更管理手順の使用によって、管理すること。

５．８．５．２　オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー

オペレーティングシステムを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要な業務用ソフトウェアをレビューし、試験すること。

５．８．５．３　パッケージソフトウェアの変更に対する制限

パッケージソフトウェアの変更は、必要な変更だけに限ること。また、すべての変更は、厳重に管理すること。

５．８．５．４　情報の漏えい

情報の漏えいの可能性を抑止すること。

５．８．５．５　外部委託によるソフトウェア開発

組織は、外部委託したソフトウェア開発を監督し、監視すること。

５．８．６　技術的ぜい弱性管理の管理目的

５．８．６．１　技術的ぜい弱性の管理

利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する

こと。また、そのようなぜい弱性に組織がさらされている状況を評価し、それと関連するリスクに対処するために、適切な手段を講じること。

５．９ 情報セキュリティインシデントの管理

５．９．１　情報セキュリティの事象及び弱点の報告の管理目的

５．９．１．１　情報セキュリティ事象の報告

一般の情報セキュリティ基本方針の内容に加え、個人ヘルスケア情報を取り扱う組織は、迅速で効果的、かつ理路整然としたセキュリティ事件への対応を確かなものとするために、セキュリティ事件管理の責任と手順を確立することが望ましい。組織は、危機管理や事業継続計画のような事件の効果的エスカレーション経路についても考慮することが望ましい。それらは的確な環境かつ的確な時間で、監査証跡やログ、そして他の証拠のような事件に関連するデータを保全したうえで発動されるものであることが望ましい。

セキュリティ事件は、改ざん、個人情報の意図しない暴露、単純にヘルスケア情報システムを使えないことを含み、それらはサービスの可用性に悪影響を及ぼすか、情報セキュリティ事件のために引き起こされる診療上の事件の原因にもなる。

組織は、個人ヘルスケア情報が、意図的であってもそうでなくても、漏洩した場合には、情報の主体である利用者本人に報告することが望ましい。

組織は、ヘルスケア情報システムの可用性の欠如が、治療の主体の過去もしくは現在の治療に悪影響を及ぼす場合には、医療機関側に報告することが望ましい。

セキュリティ評価は、全ての事件またはサンプル、それら導く確立された管理策とリスク評価に対して行われることが望ましい。

５．９．１．２　セキュリティ弱点の報告

５．９．１．１に順ずる。

５．９．２　情報セキュリティインシデントの管理及びその改善の管理目的

５．９．２．１　責任及び手順

情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするために、責任体制及び手順を確立すること。

５．９．２．２　情報セキュリティインシデントからの学習

情報セキュリティインシデントの形態、規模及び費用を定量化し監視できるようにする仕組みを備えること。

５．９．２．３　証拠の収集

個人ヘルスケア情報を取り扱う組織は、医療過誤を立証し、適切な方針を確認するための証拠収集の含蓄、そしてヘルスケア情報システムが管轄上の境界を越えてアクセス可能である場合には、管轄間における要求事項も考慮しなければならない。

５．１０ 業務継続管理

５．１０．１　事業継続管理における情報セキュリティの側面の管理目的

災害復旧を含む事業継続管理は、医療機関に対する要求事項として認識されるようになってきており、その優先度も高くなってきている。ヘルスケアにおける広範囲な可用性の要求事項を反映して、ヘルスケア要員のための教育や技術向上のために投資されることが望ましい。

５．１０．１．１　事業継続管理手続への情報セキュリティの組込み

組織全体を通じた事業継続のために、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う、管理された手続を、策定し、維持すること。

５．１０．１．２　事業継続及びリスクアセスメント

業務プロセスの中断を引き起こしうる事象は、そのような中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに、特定すること。

５．１０．１．３　情報セキュリティを組み込んだ事業継続計画の策定及び実施

重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にするために、計画を策定し、実施すること。

５．１０．１．４　事業継続計画策定の枠組み

すべての計画が整合したものになることを確実にするため、情報セキュリティ上の要求事項を矛盾なく取り扱うため、また、試験及び保守の優先順位を特定するために、一つの事業継続計画の枠組みを維持すること。

５．１０．１．５　事業継続計画の試験、維持及び再評価

事業継続計画が最新で効果的なものであることを確実にするために、定めに従って試験・更新すること。

５．１１ コンプライアンス

５．１１．１　法的要求事項の順守の管理目的

ヘルスケアにおける監査プログラムは形式的に、本附属書の全ての要素と、リスクの全ての領域をカバーする構造を持つことが望ましい。

５．１１．１．１　適用法令の識別

各情報システム及び組織について、すべての関連する法令、規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組み方を、明確に定め、文書化し、また、最新に保つこと。

５．１１．１．２　知的財産権（ＩＰＲ）

知的財産権が存在する可能性があるものを利用するとき、及び権利関係のあるソフトウェア製品を利用するときは、法令、規則及び契約上の要求事項の順守を確実にす

るための適切な手順を導入すること。

５．１１．１．３　組織の記録の保護

重要な記録は、法令、規則、契約及び業務上の要求事項に従って、消失、破壊及び改ざんから保護すること。

５．１１．１．４　個人データ及び個人情報の保護

個人ヘルスケア情報を取り扱う組織は、利用者の本人同意を管理しなければならない。また、プライバシー保護に関するルールが必要である。

５．１１．１．５　情報処理施設の誤用防止

認可されていない目的のための情報処理施設の利用を防ぐこと。

５．１１．１．６　暗号化機能に対する規則

暗号化機能は、関連するすべての協定、法令、及び規則を順守して用いること。

５．１１．２　セキュリティ方針及び標準の順守、並びに技術的コンプライアンスの管理目的

５．１１．２．１　セキュリティ方針及び標準の順守

管理者は、セキュリティ方針及び標準類への順守を達成するために、自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にすること。

５．１１．２．２　技術的コンプライアンスの点検

大規模ヘルスケア情報システムは多くの相互接続システムから構成されるので、技術的な相互接続性を目的とした適合に対して、特別な注意が払われること。

５．１１．３　情報システム監査に対する考慮事項の管理目的

５．１１．３．１　情報システム監査に対する管理策

運用システムの点検を伴う監査要求事項及び活動は、業務プロセスの中断のリスクを最小限に抑えるために、慎重に計画され、合意されること。

５．１１．３．２　情報システム監査ツールの保護

情報システム監査ツールの誤用又は悪用を防止するために、それらのツールへのアクセスは、抑制すること。

附属書 B　情報資産の明確化

地域見守り支援システムで扱う情報資産を要求定義書(暫定版)から抽出し次のカテゴリで分類する。

①電子化される情報

②電子化された情報が保存される媒体、機器

③電子化された情報が一時的に移動に用いられる媒体及びネットワーク

リスクアセスメントでは、情報がどこに保管され、管理責任者は誰か、利用者の範囲と機密性、完全性、可用性による情報資産価値を明確化する必要がある。また利用する機器、媒体、ネットワークの仕様も含めてリスクアセスメントを行う必要があるが、実システム毎に実装が異なるものであることから、情報の例とその取り扱い方の種類から保存場所の可能性、利用される機器、媒体、ネットワークが把握できる関係を示すにとどめる。ただし、取り扱う情報については正確な洗い出しは 2010 年 2 月時点では行われていない。

以下の例示では、情報の取り扱い種類に照らし合わせて、該当する情報資産が何処に保存される可能性があるか、何により移動される可能性があるのかの例として把握できるようにしているので、参考にしていただきたい。

（1）電子化される情報

情報の取り扱い方の種類と情報の例の関係から、情報資産の例示として示す。

表 B．1　電子化される情報の例

情報発生源と情報の例	情報の取り扱い			
	チーム全員が共有する情報	組織や職種を限定して共有する情報	組織内のみ共有する情報	一般的な情報
1. 医療機関				
患者基本情報、家系図	○			
紹介状（病名、薬剤、処置）		○		
退院サマリ（病名、薬剤、処置）		○		
検査結果		○		
処方情報（薬剤）		○		
訪問看護指示書・依頼書		○		

患者 ID（紐付け情報）		○		
2. 指定居宅サービス事業者				
利用者基本情報、家系図	○			
看護・介護計画書		○		
実施報告、評価書		○		
名簿・緊急連絡先			○	
訪問活動計画				○
3. 居宅介護支援事業所				
ケアプラン・支援計画書	○	○		
ケアカンファレンス資料	○			
相談記録		○		
ヘルパー活動記録		○		
名簿・緊急連絡先			○	
4.介護保険施設				
サービスメニュー				○
サービス提供記録		○		
名簿・緊急連絡先			○	
5. 自治体				
審査結果			○	
6. 近隣住民・ボランティア				
見守り情報、通報情報			○	
名簿・緊急連絡先			○	
7. 本人・家族				
同意書			○	
申請書			○	
契約書			○	
連絡ノート			○	

（2）電子化された情報が保存される媒体、機器

情報の取り扱い方の種類と媒体、機器の例の関係から、情報資産の例示として示す。

表 B．2　電子化された情報が保存される媒体、機器の例

媒体、機器の例	情報の取り扱い			
	チーム全員が共有する情報	組織や職種を限定して共有する情報	組織内のみ共有する情報	一般的な情報
1．サーバ				
見守り共有サーバ（データセンタ）	○	○		○
介護情報サーバ（施設サーバ室）			○	○
介護情報サーバ（各施設フロア）			○	○
２．PC				
デスクトップ PC			○	○
モバイル PC	○		○	○
PDA	○		○	○
３．携帯端末				
携帯電話	○			○
４．記録媒体（保存用）				
CD、DVD			○	○

（3）電子化された情報が一時的に移動に用いられる媒体及びネットワーク

可搬媒体、ネットワークの例と情報の取り扱い方の関係から、情報資産の例示として示す。

表 B．3　電子化された情報が一時的に移動に用いられる媒体及びネットワークの例

可搬媒体、ネットワークの例	情報の取り扱い			
	チーム全員が共有する情報	組織や職種を限定して共有する情報	組織内のみ共有する情報	一般的な情報
1．ネットワーク				
インターネット	○			○
インターネット（VPN）	○	○	○	○

専用線	○	○	○	○
無線 LAN			○	○
携帯電話・テレビ電話	○		○	○
ケーブルテレビ	○		○	○
FAX	○		○	○
２．可搬媒体				
USB 等の小型メモリ			○	○
モバイル PC	○		○	○
CD、DVD			○	○
３．見守り機器				
バイタルセンサ			○	

附属書Ｃ　リスクアセスメント

Ｃ．１　本附属書の目的

情報システムに実装されるべきセキュリティ機能と、その運用において実施されるべき管理策の選択は、基本的にはリスクアセスメントを実施した結果から導出されるべきものである。これらがリスクアセスメントの結果に基づいていないと、セキュリティ対策に漏れ（セキュリティホール）が発生したり、逆に過剰なセキュリティ対策によって運用上の可用性を損ねたり、対策費用が必要以上にかかったりする弊害が懸念される。

完全なリスクアセスメントを実施するためには、当該の情報システムの構成や機能、それを運用する組織の体制などがすべて正確に把握できている必要があるが、「地域見守り支援システム」については、2010 年 2 月時点において情報モデルが最終確定していない。したがって、完全なリスクアセスメントの実施は、これが確定する次年度以降の課題となる。

ただし、採用するリスクアセスメントの手法と手順については、情報モデルが最終確定していなくても制定することは可能である。これらを予め定めておくことにより、実際に「地域見守り支援システム」を構築、運用する組織が、ここでのやり方を参考とすることで、対象システムのリスクアセスメントを効果的、かつ効率的に行えるようになることが期待できる。

本附属書では、「平成 21 年度　経済産業省　地域見守り支援システム実証事業　要求定義書（暫定版）」（以下、「要求定義書」）に記載された業務シナリオの一部を対象として選び、そこから導出される典型的な情報資産について、サンプル的なリスクアセスメントを行った。

Ｃ．２　リスクアセスメントの手法

本附属書で行うリスクアセスメントの手法は、

「財団法人　日本情報処理開発協会（JIPDEC）」が発行している「ISMS ユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応--リスクマネジメント編-」（http://www.isms.jipdec.jp/doc/JIP-ISMS113-21.pdf）に記載された手法を参考とした。

Ｃ．３　情報セキュリティ基本方針

リスクアセスメントを行う際には、評価の拠り所として当該組織の情報セキュリティ基本方針が重要となる。これらは組織によって異なるので、本附属書では本書の本文である 9 章の記述から、「地域見守り支援システム」における標準的な情報セキュリ

ティ基本方針を読み取り、その考え方に従うこととした。

C．４ リスクアセスメントの実施例

上記の前提条件に従って、本附属書では、「要求定義書」（附属書 A．業務シナリオのモデル化）における「A.7　訪問看護師による見守り」をリスクアセスメントの対象とした。

C．４．１ 対象とする情報資産の抽出

上記の業務シナリオのユースケースは下記のように記述されている。

表 C．４－１業務シナリオのユースケース

	項目	イベント	アクタ	シナリオ
連携調整	1-1	提供記録確認	本人、家族 看護師 ケアマネ	訪問看護ステーションの看護師は、地域見守り支援システムを使って、前日に訪問したホームヘルパーのサービス提供記録を確認している。
	1-2	状態確認	本人、家族 看護師 かかりつけ医	Ａさんが「最近は、あまり体調が良くない。食欲がない」と訴えていることを確認し、かりつけ医と相談してＡさんの病気の状態を確認することにした。
サービス提供	2-1	状況		看護師がバイタルデータを測定したところ、血圧と血糖値が低下していることがわかった。Ａさんに、空腹感や身体のだるさがないかと確認したところ、「ある」との答えだったため、低血糖の症状が疑われた。
	2-2	報告・指示依頼	本人、家族 看護師 かかりつけ医	そのため、看護師が、携帯電話を使って、かかりつけ医にＡさんの症状とバイタルデータを伝え、指示を仰いだ。
	2-3	指示受け	本人、家族 看護師 かかりつけ医	かかりつけ医から「処方されているブドウ糖を飲ませるように。無ければ、砂糖水でも構わない」との指示があったために、Ａさんにブドウ糖の場所を聞き、飲めるように準備し、病状の変化を見守ることにした。
	2-4	結果記録	本人、家族 看護師 かかりつけ医 専門医	訪問看護師は、Ａさんのバイタルデータと症状、かかりつけ医からの指示などを看護記録に残し、地域見守り支援システムを使って、かかりつけ医と中核病院の担当医からアクセスできるようにした。
課題対応	3-1	専門医に報告	本人、家族 かかりつけ医 専門医	後日、かかりつけ医が訪問診療し、テレビ電話を使って中核病院の専門医にバイタルデータと現在の病状を報告。
	3-2	精密検査	本人、家族 かかりつけ医 専門医	念のために、中核病院で精密検査することになった。

表 C. ４－２ 資産のリストアップ

資産番号	情報資産名	種別	所在
A1	地域見守り支援システム	システム	データセンタ
A2	サービス提供記録	電子情報	地域見守り支援システム
A3	バイタルデータ測定機器	情報機器	訪問看護師が所持
A4	バイタルデータ	電子情報	地域見守り支援システム
A5	携帯電話	情報機器	訪問看護師が所持
A6	看護記録（紙）	紙情報	訪問看護師が所持
A7	看護記録（電子）	電子情報	地域見守り支援システム
A8	テレビ電話	情報機器	患者の自宅

リスクアセスメントは、すべての情報資産について個別に行うことが理想であるが、情報システムの規模が大きくなるにつれて、情報資産の数は飛躍的に増大するため、非常に多大な作業となってしまう。これを省力化するために、グループ分けという概念を導入する。情報の種別（形態）や重要度、管理場所等によって分類し、同じグループに属する情報資産には、同じリスクが存在すると考えるのである。

ここではサンプル的に上記を「種別」と「所在」という観点でグループ分けすると、下記のようになる。

表 C. ４－３　グループ分けの例

Gr 番号	種別	所在	該当する情報資産
G1	システム	データセンタ	A1
G2	電子情報	地域見守り支援システム	A2 A4 A7
G3	情報機器	訪問看護師が所持	A3 A5
G4	紙情報	訪問看護師が所持	A6
G5	情報機器	患者の自宅	A8

実際のグループ分けは、上記の観点だけでは粗すぎる可能性があり、もっと細かな観点（たとえば、個人情報を含むかどうか、現状施されている管理策の詳細な相違など）を加える必要があるかもしれないが、考え方としては同じである。

ここでのリスクアセスメントは、これらグループごとに実施した。

C. ４．2 想定される脅威

上記で抽出したそれぞれの情報資産（のグループ）に対し、想定される脅威を考え

る。情報セキュリティでのリスクの観点は、機密性（C)、完全性（I)、可用性（A）の３つである。地域見守り支援のビジネスとしては、患者の安全性、システム運用の経済性等、より広い観点でのリスクも考えられるが、ここではこれらは対象としない。

ここで留意すべきことは、脅威の抽出の際に評価をしないということである。すなわち、その脅威の発現の頻度が低いからと言って、最初から除外しないということである。これはリスク分析を実施した担当者と、組織の経営陣のリスクに対する評価が異なる可能性があるからである。抽出の際に実施者によるフィルタリングがかかっていると、リスク分析が正確に行われない可能性がある。したがって、このようなフィルタリングの作業は後の「リスク評価」のところで行う。

脅威は、その情報資産の固有の管理状況に大きく依存するため、ここでは通常考えられる代表的なもののうち、ごく一部の抽出に留めた。実際に脅威を抽出する際には、それぞれの組織の実態に合わせて行う必要がある。

表 C. ４－４　脅威のリストアップ

Gr 番号	脅威番号	観点	脅威の内容
G1	T1-I1	I	非作為的な事故により DB が壊れる
	T1-A1	A	通信回線の定期保守により利用できない
	T1-A2	A	利用者による負荷が集中しシステムの応答が遅くなる
G2	T2-C1	C	何者かに不正に閲覧される
	T2-I1	I	何者かによって内容が削除または改ざんされる
	T2-I2	I	利用者が操作を誤ってデータを消してしまう
	T2-A1	A	システムの定期保守によりアクセスできなくなる
G3	T3-C1	C	何者かに不正に操作される
	T3-I1	I	何らかの理由により正確な測定が行えない
	T3-A1	A	機器の扱い方がわからない
	T3-A2	A	紛失する
G4	T4-C1	C	何者かに不正に閲覧される
	T4-I1	I	物理的に破損して読めなくなる
	T4-A1	A	紛失する
G5	T5-I1	I	何らかの理由により通信ができない
	T5-A1	A	機器の扱い方がわからない

ここでは「何らかの理由により」とか「何者かによって」という表現を使った部分があるが、これをより具体的な表現とすることで、リスク分析の精度はより向上する。

C. ４．3 ぜい弱性

次に、上記で抽出した、想定される脅威に関して、現在の管理策（想定）を踏まえ

たぜい弱性の一部を、下記のようにサンプル的に抽出した。

表 C. ４－５　脅威に対するぜい弱性のリストアップ

脅威番号	ぜい弱性番号	ぜい弱性	現在の管理策
T1-I1	F1-I1-1	DB を保存する記憶媒体が通常運用で壊れうる	１日１回のバックアップ
	F1-I1-2	火災により焼失する	サーバ室の消火設備
T1-A1	F1-A1-1	通信回線が使えないとシステムにアクセスできない	計画保守スケジュールを利用者に周知
T1-A2	F1-A2-1	サーバの処理能力に限界がある	特になし
T2-C1	F2-C1-1	ぜい弱なパスワードを使用している	特になし(パスワードの設定ポリシーを定めず、ユーザに委ねている)
T2-I1	F2-I1-1	共有アカウントが利用されている	特になし(共有アカウントに関する規制がない)
T2-I2	F2-I2-1	誤操作に対する警告機能がない	特になし
T2-A1	F2-A1-1	システムを定期的に停止しなければならない	計画保守スケジュールを利用者に周知
T3-C1	F3-C1-1	パスワードを設定できない	特になし
T3-I1	F3-I1-1	定期的な補正が必要	特になし
T3-A1	F3-A1-1	使い方が複雑	操作マニュアルを配布
T3-A2	F3-A2-1	小型軽量なので簡単に持ち運びができる	特になし
T4-C1	F4-C1-1	通常の書架に保管しているため誰でも閲覧できる	特になし
T4-I1	F4-I1-1	原本しかない	特になし
T4-A1	F4-A1-1	通常のバッグに入れて持ち歩いている	特になし
T5-I1	F5-I1-1	通信回線の定期メンテナンスがある	計画保守スケジュールを利用者に周知
T5-A1	F5-A1-1	お年寄りが使っている	操作マニュアルを配布

C. ４．４ リスク値の計算

上記で情報資産およびそれぞれに関する脅威とぜい弱性が抽出できたので、次はこれらを定量的に評価することで、リスクの大きさ（実際に脅威が発顕する可能性）を計算する。

ここでは JIPDEC の「ISMS ユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応--リスクマネジメント編-」での例示を基に評価を行う。基本的には結果のみを示すので、そこに至った考え方などの詳細については、同書を参考して自組

織の現状に合わせる必要がある。

（1）情報資産の価値

上記にリストアップした情報資産について、その価値を算定する場合には、資産の価値を評価するよりも、資産の機密性（A)、完全性（I)、可用性（A）が損なわれた場合の事業上の影響（損害）を評価するとした方が考えやすい。

この考えに沿って、JIPDEC のガイドでは、下記のような例が示されている。自組織に合ったものを選択してそのまま使ってもよいし、適宜修正して使ってもよい。

表 C. ４－６　機密性の評価基準例

資産価値	クラス	説明
1	公開	内容が漏えいした場合でも、ビジネスへの影響はほとんどない
2	社外秘	内容が漏えいした場合、ビジネスへの影響は少ない
3	秘密	内容が漏えいした場合、ビジネスへの影響は大きい
4	極秘	内容が漏えいした場合、ビジネスへの影響は深刻かつ重大である

表 C. ４－７　影響度の評価基準例

資産価値	影響度	金銭・機会損失（短期）	金銭・機会損失（中長期）	信用・ブランド損失
1	非常に小さい	当期経営にはほとんど影響はない	中長期的な経営には影響はない	ほとんど影響はない
2	小さい	当期経営に軽微な影響（追う気利益の 1%以下）を及ぼす	中長期的な影響はない	弦された人に対して悪い風評が及ぶ
3	中程度	当期経営に影響（当期利益の 3%以下）を及ぼす	中長期的な経営にはほとんど影響はない	多くの人に対して悪い風評が及ぶ
4	大きい	当期経営に重大な影響（当期利益の 10%未満）を及ぼす	2 年程度の経営に影響が及ぶ	限定された人に長期的に悪いイメージが残る
5	非常に大きい	当期経営に極めて重大な影響（当期利益の 10%以上）を及ぼす	3 年以上の経営に影響が及ぶ	多くの人に対し長期的に悪いイメージが残る

（2）脅威の評価

脅威の評価に関しては、単純な発生頻度によるもの、脅威の発生用によるものが示されている。自組織に合ったものを選択してそのまま使ってもよいし、適宜修正して使ってもよい。

表 C. ４－８　脅威の分類基準例（１）

脅威		
レベル	区分	説明
1	低い	発生する可能性は低い。発生頻度は 1 年に 1 回あるかないかである。
2	中程度	発生する可能性は中程度である。発生頻度は半年以内に 1 回あるかないかである。
3	高い	発生する可能性は高い。発生頻度は 1 ヶ月に 1 回以上である。

表 C. ４－９　脅威の分類基準例（２）

脅威			
レベル	意図的（計画的）脅威	偶発的脅威	環境的脅威
1	実施による利益はない	通常では発生しない	3 年以内に一度も発生しない
2	実施による利益はあまりない	特定の状況下での発生が考えられる	3 年に一度程度発生する
3	実施による利益は多少ある	専門能力のあるものの不注意で発生する	1 年に一度程度発生する
4	実施による利益がある	一般者の不注意で発生する	1 ヶ月に一度程度発生する
5	発生が具体的に予想される	通常の状態で発生する	1 ヶ月に一度以上発生する

（３）ぜい弱性の評価

ぜい弱性の評価は、その資産の持つ弱点がどの程度であるかを評価することになる。すなわち、現在実施されている対策を考慮して、ぜい弱性の評価を行うことになる。表現は脅威の場合と同様のものが示されている。

表 C. ４－１０　ぜい弱性の分類基準例（１）

ぜい弱性		
レベル	区分	説明
1	低い	現状の対策でほぼ完全に防御できる。
2	中程度	現在の対策で、かなりの場合防御可能であるが、万全とは言えない。
3	高い	現在の対策では、ほとんど防御できない。

表 C. ４－１１　ぜい弱性の分類基準例（２）

ぜい弱性			
レベル	意図的（計画的）脅威 に対するぜい弱性	偶発的脅威 に対するぜい弱性	環境的脅威 に対するぜい弱性
1	最高程度の対策を実施済み	最高程度の対策を実施済み	最高程度の対策を実施済み
2	高度な専門知識や設備を持つ者によって可能な状況	通常の利用状況ではほとんどリスクが顕在化する恐れがない状況	通常の利用状況ではほとんどリスクが顕在化する恐れがない状況
3	専門能力を持つ者によって可能な状況	専門能力があるものの不注意によりリスクが顕在化する恐れがある状況	専門能力があるものの不注意によりリスクが顕在化する恐れがある状況
4	一般者が調査を実施すれば可能な状況	一般者の不注意によりリスクが顕在化する恐れがある状況	一般者の不注意によりリスクが顕在化する恐れがある状況
5	一般者が不通に実施可能な状況	特段の対策を実施しておらず、いつリスクが顕在化してもおかしくない状況	特段の対策を実施しておらず、いつリスクが顕在化してもおかしくない状況

ここでリストアップした資産（グループ)、脅威、ぜい弱性に対して、その環境を考慮して値を入れてみると下記のようになった。なお、ここでは脅威およびぜい弱性の評価に、３段階のもの（表 C. ４－８、表 C. ４－１０）を利用した。どの評価尺度を使うかは、組織の実情を考慮して決めればよい。

表 C. ４－１２　資産、脅威、ぜい弱性の評価値

Gr 番号	評価値	脅威番号	評価値	ぜい弱性番号	評価値
G1	3	T1-I1	2	F1-I1-1	2
			2	F1-I1-2	2
		T1-A1	1	F1-A1-1	2
		T1-A2	2	F1-A2-1	2
G2	4	T2-C1	1	F2-C1-1	2
		T2-I1	1	F2-I1-1	1
		T2-I2	1	F2-I2-1	1
		T2-A1	1	F2-A1-1	1
G3	1	T3-C1	1	F3-C1-1	3
		T3-I1	1	F3-I1-1	1
		T3-A1	3	F3-A1-1	2
		T3-A2	1	F3-A2-1	2
G4	2	T4-C1	2	F4-C1-1	2

		T4-I1	2	F4-I1-1	2
		T4-A1	2	F4-A1-1	2
G5	1	T5-I1	1	F5-I1-1	1
		T5-A1	2	F5-A1-1	2

リスクの値は、前の作業で明確になった「資産の価値」、「脅威の大きさ」、「ぜい弱性の度合い」を用いて、たとえば、簡易的に次のような式で算出することができる。

リスクの値　＝　「資産の価値」×「脅威の大きさ」×「ぜい弱性の度合い」

この式を用いて、表 C. ４－１２でリスク値を計算すると記のようになった。

表 C. ４－１３　リスク値の計算結果

Gr 番号	評価値	脅威番号	評価値	ぜい弱性番号	評価値	リスク値
G1	3	T1-I1	2	F1-I1-1	2	12
			2	F1-I1-2	2	12
		T1-A1	1	F1-A1-1	2	6
		T1-A2	2	F1-A2-1	2	12
G2	4	T2-C1	1	F2-C1-1	2	8
		T2-I1	1	F2-I1-1	1	4
		T2-I2	1	F2-I2-1	1	4
		T2-A1	1	F2-A1-1	1	4
G3	1	T3-C1	1	F3-C1-1	3	3
		T3-I1	1	F3-I1-1	1	1
		T3-A1	3	F3-A1-1	2	6
		T3-A2	1	F3-A2-1	2	2
G4	2	T4-C1	2	F4-C1-1	2	8
		T4-I1	2	F4-I1-1	2	8
		T4-A1	2	F4-A1-1	2	8
G5	1	T5-I1	1	F5-I1-1	1	1
		T5-A1	2	F5-A1-1	2	4

（4）リスクの評価

計算して得られたリスク値は、表 C. ４－１３のとおりである。これでそれぞれの資産に対するリスクの相対的な大きさがわかった。次はこのうちのどこまでが受容可能であるかを評価する。この結果、受容できないとなったリスクについては対策を施し、リスクを受容できるレベルにまで低減する必要がある。

この際、次のようなリスク受容の一覧表を作成すると考えやすい。

表 C. ４－１４　リスク受容一覧表

	脅威								
	1			2			3		
	ぜい弱性								
資産価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	8	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

ここで、組織の実情に合わせて、受容範囲を決める。下記のような例を参考にして決めるとよい。

受容範囲決定方針の例

資産価値が最大のものは、脅威とぜい弱性がともに最低レベルより上のものは受容しない。すなわち、＜資産価値＞＜脅威＞＜ぜい弱性＞の組み合わせが、４×２×１または４×１×２となるものとする。したがって、リスク値８未満は受容する。

上記の受容範囲決定方針に従って、表 C. ４－１４に受容範囲を表現すると下記のようになる。

表 C. ４－１５　リスク受容範囲の例

	脅威								
	1			2			3		
	ぜい弱性								
資産価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	8	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

（灰色の網掛け部分が受容可能、それ以外は何らかの対策が必要）

この評価基準を用いて表 C. ４－１３を評価すると下記のようになる。

表 C. ４－１６　リスク値の評価結果

Gr 番号	評価値	脅威番号	評価値	ぜい弱性番号	評価値	リスク値
G1	3	T1-I1	2	F1-I1-1	2	12
			2	F1-I1-2	2	12
		T1-A1	1	F1-A1-1	2	6
		T1-A2	2	F1-A2-1	2	12
G2	4	T2-C1	1	F2-C1-1	2	8
		T2-I1	1	F2-I1-1	1	4
		T2-I2	1	F2-I2-1	1	4
		T2-A1	1	F2-A1-1	1	4
G3	1	T3-C1	1	F3-C1-1	3	3
		T3-I1	1	F3-I1-1	1	1
		T3-A1	3	F3-A1-1	2	6
		T3-A2	1	F3-A2-1	2	2
G4	2	T4-C1	2	F4-C1-1	2	8
		T4-I1	2	F4-I1-1	2	8
		T4-A1	2	F4-A1-1	2	8
G5	1	T5-I1	1	F5-I1-1	1	1
		T5-A1	2	F5-A1-1	2	4

（灰色の網掛け部分が受容可能、それ以外は何らかの対策が必要）

これによると、G1 の資産については完全性と可用性の観点での対策が、G2 については機密性観点での対策が、G4 については機密性・完全性・可用性すべての対策が必要であることがわかる。

（５）管理策とリスクの再評価

リスク評価で管理策が必要となった情報資産には、何らかの対策を施して、脅威もしくはぜい弱性のレベルを低減しなければならない。このため対策のことを「管理策」と呼び、ISMS として知られる JIS Q 27001:2006(ISO/IEC 27001:2005）および「安全管理のガイドライン」などで記述されているものが利用可能である。

一般的には、脅威のレベルを下げることは難しく、管理策はぜい弱性のレベルを下げることが主体となる。資産価値が大きく、かつ脅威のレベルが高いものについては、その資産自体を廃止する（「リスクの回避」という）といった対策を考慮せざるを得ないような場合も想定されるので、注意が必要である。

何らかの有効な管理策を採用することで、脅威またはぜい弱性のレベルが下がることがわかったら、その値を用いて再度リスクの評価を行う。これを「リスクの再評価」

と呼ぶ。

表 C. ４－１６で対策が必要となった資産のぜい弱性を下げる方策の例と、それによる効果を下記に示す。

表 C. ４－１７　リスク値の評価結果

Gr 番号	ぜい弱性番号	評価値	管理策	再評価値
G1	F1-I1-1	2	ディスク構成を RAID-6 に変更する	1
	F1-I1-2	2	バックアップを別の建屋に保管する	1
	F1-A2-1	2	高速なディスクに変更する	1
G2	F2-C1-1	2	パスワードの設定方針を定める	1
G4	F4-C1-1	2	鍵付きの書架に保管する	1
	F4-I1-1	2	物理コピーを毎日とる	1
	F4-A1-1	2	携行する際のルールを定める	1

上記の管理策を施すことで、表 C. ４－１６は下記のようなり、すべてのリスクが受容可能となったことがわかる。

表 C. ４－１８　リスク値の再評価結果

Gr 番号	評価値	脅威番号	評価値	ぜい弱性番号	評価値	リスク値
G1	3	T1-I1	2	F1-I1-1	1	6
			2	F1-I1-2	1	6
		T1-A1	1	F1-A1-1	2	6
		T1-A2	2	F1-A2-1	1	6
G2	4	T2-C1	1	F2-C1-1	1	4
		T2-I1	1	F2-I1-1	1	4
		T2-A1	1	F2-A1-1	1	4
			1	F2-A1-2	1	4
G3	1	T3-C1	1	F3-C1-1	3	3
		T3-I1	1	F3-I1-1	1	1
		T3-A1	3	F3-A1-1	2	6
		T3-A2	1	F3-A2-1	2	2
G4	2	T4-C1	2	F4-C1-1	1	4
		T4-I1	2	F4-I1-1	1	4
		T4-A1	2	F4-A1-1	1	4
G5	1	T5-I1	1	F5-I1-1	1	1
		T5-A1	2	F5-A1-1	2	4

（灰色の網掛け部分が受容可能、それ以外は何らかの対策が必要）

（6）経営陣による残留リスクの承認

表 C. ４－１８に示したように、新たな管理策を施すことで、すべてのリスクは受容可能なレベルに下がったことが確認できたが、リスクが全くなくなったわけではない。このように、対策を行ってもまだ残るリスクのことを「残留リスク」という。
残留リスクが具体的にどのようなリスクであるかを下記に示す。

表 C. ４－１９　残留リスクの具体的な内容の例

Gr 番号	脅威番号	ぜい弱性番号	リスク値	残留リスクの具体な内容
G1	T1-I1	F1-I1-1	6	RAID-6 構成でも復旧できないディスク障害が発生し、障害発生時点から前日バックアップ時点までのデータが失われる
		F1-I1-2	6	同上、およびサービス再開までの時間と費用が大きなものになる
	T1-A1	F1-A1-1	6	通信回線の復旧までに予想以上の時間がかかり、利用者への影響が大きくなる
	T1-A2	F1-A2-1	6	混雑時にシステムの応答が遅くなり、利用者への影響が出る
G2	T2-C1	F2-C1-1	4	設定方針の遵守をシステム機能でなく運用ルールで担保することで、ルールを遵守しない利用者のパスワードが破られて個人情報が漏えいする
	T2-I1	F2-I1-1	4	利用方針の遵守をシステム機能でなく運用ルールで担保することで、ルールを遵守しない利用者の操作が追跡できなくなる
	T2-I2	F2-I2-1	4	誤ってデータを消してしまった利用者から、操作性の悪さに関するクレームが寄せられる
	T2-A1	F2-A1-1	4	計画保守スケジュールの通知漏れにより、利用者からクレームが寄せられる
G3	T3-C1	F3-C1-1	3	紛失もしくは盗難にあった機器からシステムに不正アクセスされる
	T3-I1	F3-I1-1	1	機器の測定誤差により、不適切なバイタルデータをアップしてしまう
	T3-A1	F3-A1-1	6	機器の操作に不慣れな操作員に対する利用者からのクレームが寄せられる
	T3-A2	F3-A2-1	2	所定のサービスが行えず、利用者からのクレームが寄せられる、利用者の個人情報が漏えいする
G4	T4-C1	F4-C1-1	4	書類の置き忘れ、盗難等により利用者の個人情報が漏えいする

	T4-I1	F4-I1-1	4	所定のサービスが行えず、利用者からのクレームが寄せられる
	T4-A1	F4-A1-1	4	所定のサービスが行えず利用者からのクレームが寄せられる、または利用者の個人情報が漏えいする
G5	T5-I1	F5-I1-1	1	所定のサービスが行えず利用者からのクレームが寄せられる
	T5-A1	F5-A1-1	4	所定のサービスが行えず利用者からのクレームが寄せられる

これらの残留リスクは、リスクアセスメントの結果からは「発生頻度が十分に低い」もしくは「発生しても被害が小さい」等の理由で「受容可能」となったものであるが、内容を見る限りでは、必ずしも放置して良いものばかりとは言えないはずである。
経営陣は、これらの残留リスクが存在することを容認できるかどうか、再度検討しなければならない。容認できないと結論した場合には、さらなる対策を行い、容認できるレベルにまで低減する必要がある。中には効果的な低減策が立案できないものもあるであろう。そういう場合には、損害を見越して保険をかける（リスクファイナンス）ことや、資産そのものの利用をやめる（リスクの回避）などの方策を講じることも検討する必要がある。

そして、いったん容認した後には、万一それらが発現した際の責任と対応を考えておく必要がある。

附属書 D　運用マニュアル例

（次年度、各地域実証事業を調査し、その結果を基に作成する。）

引用規格･引用文献

[1]　ISO/IEC 27001、27002
[2]　医療情報システムの安全管理に関するガイドライン　第4版　2009年3月　厚生労働省
[3]　医療情報を受託管理する情報処理事業者向けガイドライン　経済産業省
[4]　ASP･SaaSにおける情報セキュリティ対策ガイドライン　総務省
[5]　ASP･SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン　総務省
[6]　SaaS向けSLAガイドライン　経済産業省
[7]　ガイドラインの実装事例に関する報告書　保健･医療･福祉情報セキュアネットワーク基盤普及促進コンソーシアム（HEASNET）
[8]　ICF国際生活機能分類―国際障害分類改定版―　世界保健機構（WHO）